R E P U B L I Q U E F R A N Ç A I S E

10/089646 #3

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 27 MARS 2002

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

M Hauc

Martine PLANCHE

CERTIFIED COPY OF
PRIORITY DOCUMENT

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (1) 53 04 53 04
Télécopie : 33 (1) 42 93 59 30
www.inpi.fr

THIS PAGE BLANK (USPTO)

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES

N° D'ENREGISTREMENT NATIONAL

DÉPARTEMENT DE DÉPÔT 21 JUIL 2000
35 INPI RENNES

DATE DE DÉPÔT 21 JUIL. 2000

0009644

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Patrice VIDON
Cabinet Patrice VIDON
Immeuble Germanium
80 avenue des Buttes de Coësmes
35700 RENNES

n°du pouvoir permanent | références du correspondant 6581 | téléphone 02.99.38.23.00

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire

☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

Procédé et système d'authentification dynamique

3 DEMANDEUR (S) n° SIREN . . . . . code APE-NAF . . . .

Nom et prénoms (souligner le nom patronymique) ou dénomination — Forme juridique

1. **FRANCE TELECOM** — **Société Anonyme**
2. **TELEDIFFUSION DE FRANCE** — **Société Anonyme**
3. **MathRiZK** — **SPRL (Société de droit belge)**

Nationalité (s): Française (1,2) Belge (3)

Adresse (s) complète (s) — Pays

1. 6 place d'Alleray, 75015 PARIS — France (1,2)
2. 10, rue d'Oradour-sur-Glane, 75732 PARIS Cédex 15 — France (1,2)
3. Verte Voie, 20 – Boîte 5, B-1348 LOUVAIN-LA-NEUVE, Belgique — Belgique (3)

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande
France	99 12465	1er octobre 1999	
France	99 12467	1er octobre 1999	
France	99 12468	1er octobre 1999	

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

P. VIDON
(CPI 92-1250)

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION — SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

LE DANVIC

Description

Les objectifs des schémas GQ sont l'authentification dynamique d'entités et de messages ainsi que la signature numérique de messages. Ce sont des schémas « sans transfert de connaissance ». Une entité prouve : elle connaît un ou plusieurs nombres privés. Une autre entité contrôle : elle connaît le ou les nombres publics correspondants. L'entité qui prouve veut convaincre l'entité qui contrôle sans révéler le ou les nombres privés, de façon à pouvoir les utiliser autant de fois que de besoin.

Chaque schéma GQ repose sur un module public composé de grands nombres premiers secrets. Un exposant public v et un module public n forment ensemble une clé de vérification $\langle v, n \rangle$ signifiant « élever à la puissance v modulo n » et mise en œuvre au moyen d'une ou plusieurs équations génériques, toutes du même type, direct : $G \equiv Q^v \pmod{n}$ ou inverse : $G \times Q^v \equiv 1 \pmod{n}$. Le type a un effet sur le déroulement des calculs au sein de l'entité qui contrôle, pas au sein de l'entité qui prouve ; en fait, les analyses de sécurité confondent les deux types. Chaque équation générique lie un nombre public G et un nombre privé Q formant ensemble un couple de nombres $\{G, Q\}$. En résumé, chaque schéma GQ met en œuvre un ou plusieurs couples de nombres $\{G, Q\}$ pour la même clé $\langle v, n \rangle$.

Une version classique de schémas GQ, appelée ici GQ1, fait appel à un schéma RSA de signature numérique. La clé de vérification $\langle v, n \rangle$ est alors une clé publique RSA où l'exposant v impair est de préférence un nombre premier. Chaque schéma GQ1 utilise en général un seul couple de nombres $\{G, Q\}$: le nombre public G est déduit de données d'identification selon un mécanisme de format qui fait partie intégrante du schéma RSA de signature numérique. Le nombre privé Q ou bien son inverse modulo n est une signature RSA des données d'identification. L'entité qui prouve démontre la connaissance d'une signature RSA de ses propres données d'identification et cette preuve ne révèle pas la signature qui reste donc secrète pour être

utilisée autant de fois que de besoin.

Les schémas GQ1 mettent généralement en œuvre deux niveaux de clés : la clé privée de signature RSA est réservée à une autorité accréditant des entités se distinguant les unes des autres par des données d'identification. On dit qu'un tel schéma est « basé sur l'identité ». Ainsi, un émetteur de cartes à puce utilise sa clé privée RSA à l'émission de chaque carte pour calculer un nombre privé Q qu'il inscrit comme clé privée diversifiée dans la carte ; ou encore, un client sur un réseau d'ordinateurs utilise sa clé privée RSA à chaque entrée en session pour calculer un nombre privé Q qui sera la clé privée éphémère du client durant la session. Les entités qui prouvent, cartes à puce ou clients en session, connaissent une signature RSA de leurs données d'identification ; elles ne connaissent pas la clé privée RSA qui, dans la hiérarchie des clés, se trouve au niveau immédiatement supérieur. Cependant, une authentification dynamique d'entités par GQ1 avec un module de 768 bits au niveau d'une autorité demande à peu près la même charge de travail qu'une authentification dynamique d'entités par RSA avec un module de 512 bits à trois facteurs premiers au niveau de chaque entité, ce qui permet à l'entité qui prouve d'utiliser la technique des restes chinois en calculant un résultat modulo chacun des facteurs premiers avant de calculer un résultat modulo leur produit.

Toutefois, la hiérarchie de clés entre une autorité et les entités accréditées n'est pas obligatoire. On peut utiliser GQ1 avec un module propre à l'entité qui prouve, ce qui permet d'utiliser la technique des restes chinois pour réduire les charges de travail de l'entité qui prouve, ce qui ne change pas fondamentalement la charge de travail de l'entité qui contrôle, mis à part le fait qu'un module au niveau de l'entité qui prouve peut être plus court qu'un module au niveau de l'autorité, par exemple 512 bits comparés à 768 bits.

Lorsque l'entité connaît les facteurs premiers de son propre module, pourquoi faire appel à un schéma RSA de signature numérique ??

Une autre version de schémas GQ, appelée ici GQ2 élémentaire, fait appel directement au problème de la factorisation d'un module n. Dans ce contexte, « directement » signifie « sans faire appel à la signature RSA ». L'objectif de GQ2 est bien de réduire les charges de travail, non seulement de l'entité qui prouve mais aussi de l'entité qui contrôle. L'entité qui prouve démontre la connaissance d'une décomposition de son propre module et cette preuve ne révèle pas la décomposition qui reste donc secrète pour être utilisée autant de fois que de besoin. La sécurité du protocole GQ2 est équivalente à la factorisation du module.

Chaque entité qui prouve dispose de son propre module n. Chaque schéma GQ2 met en œuvre un paramètre k, petit nombre plus grand que 1 fixant un exposant public $v = 2^k$, et un ou plusieurs couples de nombres $\{G_1, Q_1\}$ à $\{G_m, Q_m\}$. Chaque nombre public G_i est le carré d'un petit nombre g_i plus grand que 1 et appelé « nombre de base ». Toutes les entités qui prouvent peuvent utiliser le ou les mêmes nombres publics G_1 à G_m. La factorisation du module n et le ou les nombres privés Q_1 à Q_m sont alors au même niveau dans la hiérarchie des clés. Chaque jeu de clés GQ2 élémentaires est défini par deux conditions nécessaires et suffisantes.

- Pour chaque nombre de base, aucune des deux équations $x^2 \equiv \pm g_i \pmod{n}$ n'a de solution en x dans l'anneau des entiers modulo n, c'est-à-dire que les nombres $\pm g_i$ sont deux résidus non quadratiques modulo n.
- Pour chaque nombre de base, l'équation $x^v \equiv g_i^2 \pmod{n}$ où $v = 2^k$ a des solutions en x dans l'anneau des entiers modulo n. Le nombre privé Q_i ou son inverse modulo n est n'importe laquelle de ces solutions.

Compte tenu de la deuxième condition, pour que les nombres $\pm g_i$ soient deux résidus non quadratiques modulo n, le module n doit comporter au moins deux facteurs premiers congrus à 3 (mod 4) par rapport auxquels le symbole de Legendre de g_i diffère. Par conséquent, tout module composé de facteurs premiers dont aucun ou un seul est congru à 3 (mod 4) ne permet

pas d'établir un jeu de clés GQ2 élémentaires, ce qui privilégie les facteurs premiers congrus à 3 (mod 4). Or en prenant au hasard des grands nombres premiers, il s'avère qu'ils sont environ pour moitié congrus à 3 (mod 4) et pour moitié à 1 (mod 4). De ce fait, beaucoup de modules RSA en usage ne permettent pas d'établir des jeux de clés GQ2 élémentaires.

Nous introduisons ici les jeux de clés GQ2 généralisées pour surmonter cette limitation afin de pouvoir utiliser des techniques GQ2 avec n'importe quel module, en particulier, n'importe quel module RSA ; ils reposent sur deux principes nécessaires et suffisants.

Le premier principe reproduit la deuxième condition de GQ2 élémentaire.

— Pour chaque nombre de base g_1 à g_m, l'équation $x^v \equiv g_i^2 \pmod{n}$ où $v = 2^k$ a des solutions en x dans l'anneau des entiers modulo n.

Parce que le nombre privé Q_i ou bien son inverse modulo n est une solution à l'équation, $k-1$ carrés successifs modulo n le transforment en un nombre q_i qui est une racine carrée de G_i dans l'anneau des entiers modulo n. Selon que le nombre q_i est égal à l'un des deux nombres g_i ou $n-g_i$, ou différent des deux nombres g_i et $n-g_i$, nous disons qu'il est trivial ou non. Lorsqu'un nombre q_i est non trivial, n qui divise $q_i^2-g_i^2$ ne divise ni q_i-g_i ni q_i+g_i. Tout nombre q_i non trivial révèle donc une décomposition du module n.

$$n = \text{pgcd}(n, q_i-g_i)\times\text{pgcd}(n, q_i+g_i)$$

Le deuxième principe élargit la première condition de GQ2 élémentaire.

— Parmi les nombres q_1 à q_m, au moins un nombre q_i est non trivial.

Observons que si un nombre q_i existe alors que les nombres $\pm g_i$ sont deux résidus non quadratiques dans l'anneau des entiers modulo n, le nombre q_i est manifestement non trivial. Ainsi, les jeux de clés GQ2 élémentaires font bien partie des jeux de clés GQ2 généralisées qui permettent d'utiliser n'importe quel module, c'est-à-dire toute composition de grands nombres premiers congrus indifféremment à 3 ou à 1 (mod 4) dont au moins deux sont distincts. Par contre, beaucoup de jeux de clés GQ2 généralisées ne

sont pas des jeux de clés GQ2 élémentaires. Chaque jeu de clés GQ2 généralisées est dans l'un des deux cas suivants.

- Lorsque les $2\times m$ nombres $\pm g_1$ à $\pm g_m$ sont tous des résidus non quadratiques, c'est un jeu de clés GQ2 élémentaires.
- Lorsque parmi les $2\times m$ nombres $\pm g_1$ à $\pm g_m$, il y a au moins un résidu quadratique, ce n'est pas un jeu de clés GQ2 élémentaires; c'est ce que nous appelons ici un jeu de clés GQ2 complémentaires.

La présente invention porte sur les jeux de clés GQ2 complémentaires, par définition, ces jeux de clés GQ2 généralisées qui ne sont pas élémentaires. Outre les deux principes précédents, un tel jeu doit satisfaire un troisième principe.

— Parmi les $2\times m$ nombres $\pm g_1$ à $\pm g_m$, il y a au moins un résidu quadratique.

Pour appréhender le problème et comprendre la solution que nous en donnons, c'est-à-dire l'invention, analysons d'abord la décomposition du module n révélée par un nombre q non trivial, puis rappelons la technique des restes chinois, puis, la notion de rang dans un corps de Galois CG(p) ; puis, étudions les fonctions « élever au carré » dans CG(p) et « prendre une racine carrée » d'un résidu quadratique dans CG(p) ; enfin, analysons l'applicabilité des trois principes énoncés ci-dessus.

Analyse des décompositions du module — De même que le module n se décompose en f facteurs premiers p_1 à p_f, l'anneau des entiers modulo n se décompose en f corps de Galois CG(p_1) à CG(p_f). Dans chaque corps, il y a deux racines carrées de l'unité, à savoir ± 1. Dans l'anneau, il y a donc 2^f racines carrées de l'unité. Chaque nombre privé Q_1 à Q_m définit un nombre $\Delta_i = q_i / g_i \pmod n$ qui est une de ces 2^f racines carrées de l'unité dans l'anneau ; en d'autres termes, n divise Δ_i^2-1.

- Lorsque q_i est trivial, c'est-à-dire $\Delta_i = \pm 1$, n divise Δ_i-1 ou bien Δ_i+1 et donc Δ_i ne révèle pas de décomposition du module n.
- Lorsque q_i est non trivial, c'est-à-dire $\Delta_i \neq \pm 1$, n ne divise ni Δ_i-1 ni Δ_i+1

et donc Δ_i révèle une décomposition, n = pgcd(n, Δ_i−1)×pgcd(n, Δ_i+1), résultant de la valeur de Δ_i dans chaque corps : le ou les facteurs premiers divisant Δ_i−1 d'un côté, celui ou ceux divisant Δ_i+1 de l'autre.

Examinons les règles de composition multiplicative des nombres q. Deux nombres $\{q_1, q_2\}$ donnent un nombre composé $q_1 \times q_2$ (mod n).

- Lorsque q_1 est non trivial et q_2 trivial, le nombre composé $q_1 \times q_2$ (mod n) est non trivial ; il révèle la même décomposition que q_1.
- Lorsque q_1 et q_2 sont non triviaux et $\Delta_1 = \pm\Delta_2$, le nombre composé $q_1 \times q_2$ (mod n) est trivial ; il ne révèle pas de décomposition.
- Lorsque q_1 et q_2 sont non triviaux et $\Delta_1 \neq \pm\Delta_2$, le nombre composé $q_1 \times q_2$ (mod n) est non trivial ; il révèle une troisième décomposition.

Trois nombres $\{q_1, q_2, q_3\}$ donnent quatre nombres composés $\{q_1 \times q_2, q_1 \times q_3, q_2 \times q_3, q_1 \times q_2 \times q_3$ (mod n)$\}$, soit un total de sept nombres ; m nombres donnent ainsi $2^m - m - 1$ nombres composés, soit un total de $2^m - 1$ nombres.

Considérons un jeu de clés GQ2 généralisées comportant i nombres de base g_1 à g_i et i nombres privés Q_1 à Q_i donnant i nombres q_1 à q_i et donc i nombres Δ_1 à Δ_i qui sont des racines de l'unité. Cherchons à prendre en compte un autre nombre de base g_{i+1} par un nombre privé Q_{i+1} donnant un nombre q_{i+1} et donc une racine Δ_{i+1}.

• Le total des $2^{i+1} - 1$ nombres comporte autant de nombres non triviaux dans chacun des deux cas suivants.

- La racine Δ_{i+1} est triviale et au moins une racine Δ_1 à Δ_i est non triviale.
- La racine Δ_{i+1} est non triviale et figure parmi les $2 \times i$ racines $\pm\Delta_1$ à $\pm\Delta_i$.

• Dans le cas où la racine Δ_{i+1} est non triviale et ne figure pas parmi les $2 \times i$ racines $\pm\Delta_1$ à $\pm\Delta_i$, chaque nombre composé où figure q_{i+1} est non trivial.

Par conséquent, lorsque parmi m nombres q_1 à q_m, au moins un est non trivial, plus de la moitié du total des $2^m - 1$ nombres sont non triviaux.

Par définition, nous disons que $l < f$ nombres non triviaux $\{q_1, q_2, \cdots q_l\}$ sont <u>indépendants</u> par rapport au module n lorsque chacun des $2^l - l - 1$

nombres composés correspondants est non trivial, c'est-à-dire que, au total, les 2^l-1 nombres sont tous non triviaux. Chacun de ces 2^l-1 nombres révèle alors une décomposition différente du module n.

- Lorsque les f facteurs premiers sont distincts, il y a $2^{f-1}-1$ décompositions du module n. Alors, si $f-1$ nombres q sont indépendants, il y a une correspondance biunivoque entre les $2^{f-1}-1$ décompositions et un total de $2^{f-1}-1$ nombres comprenant les $f-1$ nombres indépendants et les $2^{f-1}-f$ nombres composés correspondants.

Restes chinois — Soient deux nombres a et b premiers entre eux tels que $0 < a < b$, et deux nombres X_a de 0 à $a-1$ et X_b de 0 à $b-1$; il s'agit de déterminer le nombre unique X de 0 à $a \times b-1$ tel que $X_a \equiv X \pmod{a}$ et $X_b \equiv X \pmod{b}$. Le nombre $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$ est le paramètre des restes chinois. Voici l'opération élémentaire des restes chinois.

$x \equiv X_b \pmod{a}$

$y = X_a - x$; si y est négatif, remplacer y par $y+a$

$z \equiv \alpha \times y \pmod{a}$

$X = z \times b + X_b$

En résumé, nous écrivons : $X =$ Restes Chinois (X_a, X_b).

Lorsque f facteurs premiers sont rangés dans l'ordre croissant, du plus petit p_1 au plus grand p_f, les paramètres des restes chinois peuvent être les suivants (il y en a un de moins que de facteurs premiers, c'est-à-dire $f-1$).

- Le premier paramètre est $\alpha \equiv (p_2 \pmod{p_1})^{-1} \pmod{p_1}$.
- Le second paramètre est $\beta \equiv (p_1 \times p_2 \pmod{p_3})^{-1} \pmod{p_3}$.
- Le i-ième paramètre est $\lambda \equiv (p_1 \times \ldots p_{i-1} \pmod{p_i})^{-1} \pmod{p_i}$.
- Et ainsi de suite.

En $f-1$ opérations élémentaires, on établit un nombre X de 0 à $n-1$ à partir de tout jeu de f composantes de X_1 à X_f avec X_j de 0 à p_j-1 :

- un premier résultat $(\text{mod } p_1 \times p_2)$ avec le premier paramètre,
- puis, un second résultat $(\text{mod } p_1 \times p_2 \times p_3)$ avec le second paramètre,

- jusqu'au résultat final (mod $n = p_1 \times p_2 \times \ldots p_f$) avec le dernier paramètre.

En résumé, étant donnés les facteurs premiers p_1 à p_f, chaque élément de l'anneau des entiers modulo n a deux représentations équivalentes :

- f nombres X_1 à X_f une composante par facteur premier : $X_j \equiv X \pmod{p_j}$,
- un nombre X de 0 à $n-1$, X = Restes Chinois $(X_1, X_2, \ldots X_f)$.

Rang des nombres dans CG(p) — Soit un nombre premier impair p et un nombre a plus petit que p, c'est-à-dire $0 < a < p$. Par définition, le rang de a par rapport à p est la période de la suite $\{X\}$ définie par $\{x_1 = a$; puis, pour $i \geq 1$, $x_{i+1} \equiv a \times x_i \pmod{p}\}$. Grâce au théorème de Fermat, nous obtenons : $x_{i+p} \equiv a^p \times x_i \equiv a \times x_i \equiv x_{i+1} \pmod{p}$. Par conséquent, le rang d'un nombre a par rapport à un nombre premier p est $p-1$ ou un diviseur de $p-1$.

Par exemple, lorsque $(p-1)/2$ est un nombre premier impair p', le corps de Galois CG(p) comporte un nombre de rang 1 : c'est 1, un nombre de rang 2 : c'est -1, $p'-1$ nombres de rang p' et $p'-1$ nombres de rang $2 \times p' = p-1$.

Dans CG(p), tout nombre de rang $p-1$ est un « générateur ». La dénomination est due au fait que les puissances successives d'un générateur dans CG(p), c'est-à-dire les termes de la suite $\{X\}$ pour les indices de 1 à $p-1$, forment une permutation de tous les éléments non nuls de CG(p).

Soit un générateur y de CG(p). Evaluons le rang du nombre $y^i \pmod{p}$ en fonction de i et de $p-1$. Lorsque i est premier avec $p-1$, c'est $p-1$. Lorsque i divise $p-1$, c'est $(p-1)/i$. Dans tous les cas, c'est $(p-1)/\text{pgcd}(p-1, i)$.

Par définition, la fonction d'Euler $\varphi(n)$ est le nombre de nombres plus petits que n et premiers avec n. Dans CG(p), il y a $\varphi(p-1)$ générateurs.

A titre d'illustration, le rang fait bien comprendre les bases du RSA. Le module n est le produit de f facteurs premiers p_1 à p_f avec $f \geq 2$. Pour chaque facteur premier p_j de p_1 à p_f, l'exposant public e doit être premier avec p_j-1. Alors, la clé $\langle e, p_j \rangle$ respecte le rang des éléments de CG(p_j) : elle permute les éléments de CG(p_j) ; il existe un nombre d_j, généralement le plus petit

possible, tel que p_j-1 divise $e\times d_j-1$. La clé $\langle d_j, p_j\rangle$ inverse la permutation des éléments de CG(p_j). Ces f permutations, une dans chaque corps CG(p_1) à CG(p_f), se traduisent dans l'anneau des entiers modulo n par la permutation RSA résumée par la clé publique $\langle e, n\rangle$. Il existe un nombre d, généralement le plus petit possible, tel que ppcm($p_1-1, p_2-1, \ldots p_f-1$) divise $d\times e-1$. Pour chaque facteur premier p_j de p_1 à p_f, on a $d_j \equiv d \pmod{p_j-1}$. La permutation RSA résumée par la clé publique $\langle e, n\rangle$ est inversée par la clé privée $\langle d, n\rangle$.

Carrés dans CG(p) — Définissons un nombre t tel que $p-1$ est divisible par 2^t, mais pas par 2^{t+1}. Chaque grand nombre premier figure dans une et une seule catégorie : $t=1$, $t=2$, $t=3$, $t=4$, et ainsi de suite. Si l'on considère un assez grand nombre de nombres premiers successifs, environ un sur deux figure dans la première catégorie où p est congru à 3 (mod 4), un sur quatre dans la deuxième où p est congru à 5 (mod 8), un sur huit dans la troisième où p est congru à 9 (mod 16), un sur seize dans la quatrième où p est congru à 17 (mod 32), et ainsi de suite ; en moyenne, un sur 2^t figure dans la t-ième catégorie où p est congru à $2^t+1 \pmod{2^{t+1}}$.

Parce que les nombres x et $p-x$ ont le même carré dans CG(p), la clé $\langle 2, p\rangle$ ne permute pas CG(p). La fonction « élever au carré » dans CG(p) peut se représenter par un graphe orienté où chaque élément non nul du corps trouve sa place. Analysons la structure du graphe en branches et en cycles selon la parité du rang de chaque élément.

- L'élément nul est fixe. C'est 0. Le rang n'est pas défini pour l'élément nul auquel aucun autre élément ne se rattache ; l'élément nul est isolé.
- L'élément unité est fixe. C'est 1, le seul élément de rang 1. Toutes les racines de l'unité dans CG(p) se trouvent dans la branche se rattachant à 1. Soit y un résidu non quadratique de CG(p), n'importe lequel ; la clé $\langle (p-1)/2^t, p\rangle$ transforme y en une racine 2^{t-1}-ième primitive de -1 notée par b ; en effet, on a $y^{(p-1)/2} \equiv -1 \pmod{p}$. Par conséquent, dans CG(p), les puissances de b pour les exposants de 1 à 2^{t-1} sont les 2^{t-1} racines de

l'unité autres que 1 : elles composent la branche se rattachant à 1.

- Le carré de tout élément de rang pair est un autre élément dont le rang est divisé par deux. Par conséquent, chaque élément de rang pair se place dans une branche ; chaque branche comporte un nombre de rang divisible par deux mais pas par quatre, puis, si $t \geq 2$, deux nombres de rang divisible par quatre mais pas par huit, puis, si $t \geq 3$, quatre nombres de rang divisible par huit mais pas par seize, puis, si $t \geq 4$, huit nombres de rang divisible par seize mais pas par 32, et ainsi de suite. Toutes les branches sont semblables à la branche rattachée à 1 ; les 2^{t-1} feuilles de chaque branche sont des résidus non quadratiques ; chaque branche comporte 2^t-1 éléments et se rattache à un élément de rang impair ; il y a $(p-1)/2^t$ branches qui ont toutes la même longueur t.
- Le carré de tout élément de rang impair autre que l'élément unité est un autre élément ayant le même rang. La clé $\langle 2, p \rangle$ permute l'ensemble des $(p-1)/2^t$ éléments de rang impair. La permutation se décompose en cycles de permutation. Le nombre de cycles dépend de la factorisation de $(p-1)/2^t$. Pour chaque diviseur p' de $(p-1)/2^t$, il y a un cycle comportant les $\varphi(p')$ éléments de rang p'. Rappelons que par définition, la fonction d'Euler $\varphi(p')$ est le nombre de nombres plus petits que p' et premiers avec p'. Par exemple lorsque $p' = (p-1)/2^t$ est premier, les $p'-1$ nombres de rang p' forment un grand cycle de permutation.

Les figures 1A à 1D illustrent chacune un fragment de graphe pour p congru respectivement à 3 (mod 4), 5 (mod 8), 9 (mod 16) et 17 (mod 32).

- Les feuilles sur les branches sont représentées par des ronds blancs ; ce sont des résidus non quadratiques.
- Les nœuds dans les branches sont représentés par des ronds gris ; ce sont des éléments quadratiques de rang pair.
- Les nœuds dans les cycles sont représentés par des ronds noirs ; ce sont des éléments quadratiques de rang impair.

Racines carrées dans CG(p) — Sachant que a est un résidu quadratique de CG(p), voyons comment calculer une solution à l'équation $x^2 \equiv a \pmod{p}$, c'est-à-dire « prendre une racine carrée » dans CG(p). Il y a bien sûr plusieurs façons d'obtenir le même résultat : on pourra consulter les pages 31 à 36 du livre de Henri Cohen, *a Course in Computational Algebraic Number Theory*, publié en 1993 par Springer à Berlin comme volume 138 de la série *Graduate Texts in Mathematics* (GTM 138).

Le nombre $s = (p-1+2^t)/2^{t+1}$ donne une clé $\langle s, p\rangle$ qui vaut :

$\langle (p+1)/4, p\rangle$ lorsque p est congru à 3 (mod 4),
$\langle (p+3)/8, p\rangle$ lorsque p est congru à 5 (mod 8),
$\langle (p+7)/16, p\rangle$ lorsque p est congru à 9 (mod 16),
$\langle (p+15)/32, p\rangle$ lorsque p est congru à 17 (mod 32),
et ainsi de suite.

- La clé $\langle s, p\rangle$ transforme tout élément d'un cycle en l'élément précédent dans le cycle. Lorsque a est de rang impair, c'est la solution de rang impair ; nous la nommons w. En effet, dans CG(p), w^2/a vaut a élevé à la puissance $(2\times(p-1+2^t)/2^{t+1})-1 = (p-1)/2^t$. L'autre solution est de rang pair ; c'est $p-w$.
- D'une manière générale, la clé $\langle s, p\rangle$ transforme tout résidu quadratique a en une première approximation de solution que nous nommons r. Puisque a est un résidu quadratique, la clé $\langle 2^{t-1}, p\rangle$ transforme certainement r^2/a en 1. Pour se rapprocher d'une racine carrée de a, élevons r^2/a à la puissance 2^{t-2} (mod p) pour obtenir +1 ou −1. La nouvelle approximation reste r si le résultat est +1 ou bien devient $b\times r$ (mod p) si le résultat est −1, sachant que b désigne n'importe quelle racine 2^t-ième primitive de 1 dans le corps CG(p). Par conséquent, la clé $\langle 2^{t-2}, p\rangle$ transforme la nouvelle approximation en 1. On peut encore se rapprocher en utilisant la clé $\langle 2^{t-3}, p\rangle$ et en multipliant par b^2 (mod p) s'il le faut, et ainsi de suite.

L'algorithme suivant résout l'équation. Il utilise les nombres a, b, p, r et t définis ci-dessus et deux variables : c représente les corrections successives

et w les approximations successives. Au début de l'algorithme, $c = b$ et $w = r$. A l'issue du calcul, les deux solutions sont w et $p-w$.

Pour i allant de $t-2$ à 1, répéter la séquence suivante :

- Appliquer la clé $\langle 2^i, p\rangle$ au nombre $w^2/a \pmod p$ pour obtenir +1 ou −1.
- Lorsque l'on obtient −1, remplacer w par $w \times c \pmod p$.
- Remplacer c par $c^2 \pmod p$.

Applicabilité des principes — Par définition, nous disons qu'un paramètre k, un nombre de base g et un facteur premier p sont *compatibles* lorsque l'équation $x^v \equiv g^2 \pmod p$ où l'exposant v vaut 2^k a des solutions en x dans le corps CG(p). Les nombres k et g sont petits et plus grands que 1. Le nombre p est un grand nombre premier.

- Lorsque $t = 1$, c'est-à-dire $p \equiv 3 \pmod 4$, l'équation a deux solutions.
- Lorsque $t = 2$, c'est-à-dire $p \equiv 5 \pmod 8$, selon le symbole de Legendre de g par rapport à p, l'équation a quatre solutions si $(g|p) = +1$; elle n'a pas de solution si $(g|p) = -1$.
- Lorsque $t > 2$, c'est-à-dire $p \equiv 1 \pmod 8$, soit u le nombre tel que 2^u divise le rang du nombre public $G = g^2$ par rapport à p, mais que 2^{u+1} ne le divise pas ; par conséquent, u est égal à l'un des nombres de 0 à $t-1$. L'équation n'a aucune solution si $u > 0$ et $k+u > t$; elle a 2^k solutions si $k+u \leq t$; elle a 2^t solutions si $u = 0$ et $k > t$.

Il y a donc deux types de compatibilité selon que G est dans un cycle ou bien en position appropriée dans une branche.

- Lorsque G est dans un cycle, c'est-à-dire $u = 0$ quelle que soit la valeur de k, il y a une solution de rang impair dans le cycle et des solutions de rang pair disséminées dans $\alpha = \min(k, t)$ branches consécutives rattachées au cycle, soit 2^α solutions en tout. La figure 2A illustre ce cas avec $k \geq t = 3$, c'est-à-dire un facteur premier congru à 9 (mod 16), ce qui impose $u = 0$.
- Lorsque G est en position appropriée dans une branche, c'est-à-dire

$u > 0$ et $u+k \leq t$, il y a 2^k solutions, toutes de rang pair et dans la branche. La figure 2B illustre ce cas.

Etant donné un paramètre k, il y a donc deux types de facteurs premiers selon que la valeur de t est inférieure à k ou bien supérieure ou égale à k.

- Pour tout facteur premier p_j tel que $t < k$, chaque G_i doit être dans un cycle et il n'y a pas de solution dans la branche rattachée à G_i. Définissons un nombre $\Delta_{i,j}$ qui vaut +1 ou −1 selon que g_i ou $-g_i$ est dans le cycle. Il n'y a pas de choix pour aucun des m nombres $\Delta_{1,j}$ à $\Delta_{m,j}$. La figure 3A illustre un cas $t < k$: G_i est dans un cycle avec un facteur premier p_j congru à 9 (mod 16), c'est-à-dire, $u = 0$, $t = 3$ avec $k > 3$.
- Pour tout facteur premier p_j tel que $t \geq k$, chaque G_i doit être tel que $u+k \leq t$, c'est-à-dire, ou bien dans un cycle avec $u = 0$ ou bien en position appropriée dans une branche avec $1 \leq u \leq t-k$. Définissons un nombre $\Delta_{i,j}$ qui vaut +1 ou −1 selon que $Q_{i,j}$ se trouve dans la partie de graphe rattachée à g_i ou à $-g_i$. Il y a le choix pour chacun des m nombres $\Delta_{1,j}$ à $\Delta_{m,j}$; chaque nombre $\Delta_{i,j}$ peut être individuellement basculé d'une valeur à l'autre. La figure 3B illustre un cas $t \geq k$: G_i est dans une branche avec un facteur premier p_j congru à 17 (mod 32), c'est-à-dire, $u = 1$, $t = 4$ avec $k = 3$.

Chaque jeu de f composantes $\{\Delta_{i,1} \ldots \Delta_{i,f}\}$ est une racine carrée de l'unité dans $CG(p_j)$. Cette racine est triviale ou pas selon que les f composantes sont égales ou pas ; nous disons alors que le jeu de f composantes est constant ou variable, ce qui traduit le fait que le nombre q_i est trivial ou pas. Par conséquent, lorsqu'un nombre q_i est non trivial, le jeu de f composantes $\{\Delta_{i,1} \ldots \Delta_{i,f}\}$ résume une décomposition du module. Il est donc possible de tester les principes avant de calculer les composantes privées $Q_{i,j}$.

- Lorsqu'un nombre public G_i est dans un cycle pour un facteur premier p_j, le nombre $\Delta_{i,j}$ vaut +1 ou −1 selon que g_i ou $-g_i$ est dans le cycle. Lorsque $p_j \equiv 3 \pmod 4$, c'est le symbole de Legendre : $\Delta_{i,j} = (g_i|p_j)$.

- Lorsqu'un nombre public G_i est en position appropriée dans une branche pour un facteur premier p_j, on peut déterminer la valeur à donner à $\Delta_{i,j}$ avant de calculer la composante privée $Q_{i,j}$.

Production de jeux de clés — Etant donné un paramètre k, il y a deux stratégies.

- Ou bien le générateur demande f facteurs premiers afin de déterminer m nombres de base. Les premiers nombres premiers : 2, 3, 5, 7, ... sont examinés pour évaluer leur compatibilité avec chacun des f grands facteurs premiers p_1 à p_f. Bien que $g = 2$ ne soit pas compatible avec $p \equiv 5 \pmod 8$, 2 peut entrer dans la composition d'un nombre de base. En effet, lorsque deux nombres sont en position similaire dans une branche, leur produit est plus près du cycle, tout comme un carré rapproche du cycle. On peut ainsi obtenir un nombre de base en composant des nombres qui individuellement ne conviennent pas.
- Ou bien le générateur demande m nombres de base et des caractéristiques du module telle qu'une taille en bits (par exemple, 512, 768, 1024, 1536, 2048) et un nombre de bits successifs à 1 en poids forts (par exemple, 1, 8, 16, 24, 32) afin de déterminer $f \geq 2$ facteurs premiers. Notés par g_1 g_2 ... g_m, les nombres de base figurent généralement parmi les premiers nombres premiers : 2, 3, 5, 7, 11, ... ou bien ce sont des combinaisons des premiers nombres premiers. Faute d'indication contraire, ce sont les m premiers nombres premiers : $g_1 = 2$, $g_2 = 3$, $g_3 = 5$, $g_4 = 7$, ... Notons que $p \equiv 5 \pmod 8$ n'est pas compatible avec $g = 2$. Le module n sera le produit de f facteurs premiers de tailles voisines, à savoir la taille assignée au module divisée par f.

Premier principe — Le paramètre k, chaque facteur premier p allant de p_1 à p_f et chaque nombre de base g allant de g_1 à g_m doivent être compatibles. Définissons un nombre h tel que 2^h divise le rang de g par rapport à p, alors que 2^{h+1} ne le divise pas. Pour calculer le nombre h, la procédure suivante

utilise le symbole de Legendre $(g|p)$ et un nombre b, racine 2^t-ième primitive de l'unité dans $\mathbb{G}(p)$.

- Si $(g|p) = +1$ avec $t = 1$, retourner « $h = 0$ ».
- Si $(g|p) = +1$ avec $t > 1$, appliquer la clé $\langle (p-1+2^t)/2^{t+1}, p \rangle$ à G pour obtenir un résultat appelé w.
  - Si $w = +g$, retourner « $h = 0$ ».
  - Si $w = p-g$, retourner « $h = 1$ ».
  - Sinon, mettre c à b et pour i allant de $t-1$ à 2,
    - appliquer la clé $\langle 2^i, p \rangle$ à $w/g \pmod p$ pour obtenir ± 1,
    - si -1, mettre h à i et remplacer w par $w \times c \pmod p$,
    - remplacer c par $c^2 \pmod p$.
  - Retourner « valeur de h de 2 à $t-1$ ».
- Si $(g|p) = -1$, retourner « $h = t$ ».

Rappelons que k, g et p sont incompatibles lorsque $u > 0$ avec $k+u > t$; ils sont compatibles lorsque $h = 0$ ou 1, quelle que soit la valeur de k, et également lorsque $h > 1$ avec $k+h \leq t+1$.

Second principe — Les trois procédures suivantes correspondent à différentes implémentations du second principe. Dans certaines implémentations, le second principe peut être renforcé au point d'exiger que chaque nombre q_1 à q_m soit non trivial. Le rôle des nombres de base est alors équilibré ; le fait d'équilibrer ou pas le second principe a un effet sur certains aspects de démonstration de la sécurité du schéma. Enfin, lorsqu'il y a $f > 2$ facteurs premiers distincts, parmi les m nombres $\{q_1 \ldots q_m\}$, on peut exiger qu'il y ait au moins un sous ensemble de $f-1$ nombres indépendants.

Les trois procédures utilisent $m \times f$ nombres $\delta_{i,j}$ définis comme suit.

- Lorsque p_j est tel que $t < k$, pour i allant de 1 à m, $\delta_{i,j} = \Delta_{i,j}$, c'est-à-dire $+1$ si $h_{i,j} = 0$ et -1 si $h_{i,j} = 1$.
- Lorsque p_j est tel que $t \geq k$, pour i allant de 1 à m, $\delta_{i,j} = 0$, ce qui indique que $\Delta_{1,j}$ à $\Delta_{m,j}$ peuvent être choisis en fonction du deuxième principe.

Une première procédure vérifie qu'au moins un jeu $\{\delta_{i,1} \ldots \delta_{i,f}\}$ est variable ou nul, c'est-à-dire qu'au moins un nombre q_1 à q_m est non trivial ou peut être choisi non trivial.

- Pour i allant de 1 à m et j allant de 1 à f,
  - si $\delta_{i,j} = 0$ ou $\neq \delta_{i,1}$, retourner « succès ».
- Retourner « échec ».

Une deuxième procédure vérifie que chaque jeu $\{\delta_{i,1} \ldots \delta_{i,f}\}$ est variable ou nul, c'est-à-dire que chaque nombre q_1 à q_m est non trivial ou peut être choisi non trivial.

- Pour i allant de 1 à m,
  - pour j allant de 1 à f,
    - si $\delta_{i,j} = 0$ ou $\neq \delta_{i,1}$, passer à la valeur suivante de i.
  - Retourner « échec ».
- Retourner « succès ».

Une troisième procédure vérifie que pour chaque paire de facteurs premiers p_{j1} et p_{j2} avec $1 \leq j_1 < j_2 \leq f$, il y a au moins un jeu $\{\delta_{i,1} \ldots \delta_{i,f}\}$ où $\delta_{i,j1}$ est nul ou différent de $\delta_{i,j2}$. Elle échoue manifestement lorsque m est plus petit que f–1. Lorsqu'elle réussit, parmi les m nombres q_1 à q_m, il y a au moins un ensemble de f–1 nombres indépendants par rapport aux f facteurs premiers.

- Pour j_1 allant de 1 à f–1 et pour j_2 allant de j_1+1 à f,
  - pour i allant de 1 à m,
    - si $\delta_{i,j1} = 0$ ou $\neq \delta_{i,j2}$, passer aux valeurs suivantes de j_1 et j_2.
  - Retourner « échec ».
- Retourner « succès ».

Lorsqu'une procédure échoue, le générateur de jeux de clés GQ2 suit sa stratégie parmi les deux stratégies possibles :

- changer l'un des m nombres de base en gardant les f facteurs premiers,
- changer l'un des f facteurs premiers en gardant les m nombres de base.

Troisième principe — La procédure suivante détermine si le jeu de clés

GQ2 généralisées en cours de production ou déjà produit est

- un jeu de clés GQ2 élémentaires, c'est-à-diré que les $2\times m$ nombres $\pm g_1$ à $\pm g_m$ sont tous des résidus non quadratiques,
- ou bien, un jeu de clés GQ2 complémentaires, c'est-à-dire que parmi les $2\times m$ nombres $\pm g_1$ à $\pm g_m$, il y a au moins un résidu quadratique.

La procédure utilise les deux symboles de Legendre $(g_i \mid p_j)$ et $(-g_i \mid p_j)$ pour i allant de 1 à m et pour j allant de 1 à f.

- Pour i allant de 1 à m,
  - pour j allant de 1 à f,
    - si $(g_i \mid p_j) = -1$, passer à la valeur suivante de i.
  - Retourner « jeu de clés GQ2 complémentaires ».
  - pour j allant de 1 à f,
    - si $(-g_i \mid p_j) = -1$, passer à la valeur suivante de i.
  - Retourner « jeu de clés GQ2 complémentaires ».
- Retourner « jeu de clés GQ2 élémentaires ».

Composantes privées — Pour une équation de type direct : $x^v \equiv g_i^2 \pmod{p_j}$, les calculs suivants établissent toutes les valeurs possibles de la composante privée $Q_{i,j}$. Les deux cas les plus simples et les plus courants, c'est-à-dire $t = 1$ et $t = 2$, sont suivis par le cas plus complexe, c'est-à-dire $t > 2$.

Pour $t = 1$, c'est-à-dire $p_j \equiv 3 \pmod 4$, la clé $\langle (p_j+1)/4, p_j \rangle$ donne la racine carrée quadratique de n'importe quel résidu quadratique dans $CG(p_j)$. On en déduit un nombre $s_j \equiv ((p_j+1)/4)^k \pmod{(p_j-1)/2}$, ce qui donne une clé $\langle s_j, p_j \rangle$ transformant G_i en $w \equiv G_i^{sj} \pmod{p_j}$. $Q_{i,j}$ est égal à w ou bien à p_j-w.

Pour $t = 2$, c'est-à-dire $p_j \equiv 5 \pmod 8$, la clé $\langle (p_j+3)/8, p_j \rangle$ donne la racine carrée de rang impair de n'importe quel élément de rang impair dans $CG(p_j)$. On en déduit un nombre $s_j \equiv ((p_j+3)/8)^k \pmod{(p_j-1)/4}$, ce qui donne une clé $\langle s_j, p_j \rangle$ transformant G_i en $w \equiv G_i^{sj} \pmod{p_j}$. Remarquons que $z \equiv 2^{(pj-1)/4} \pmod{p_j}$ est une racine carrée de -1 parce que 2 est un résidu non quadratique dans $CG(p_j)$. $Q_{i,j}$ est égal à w ou bien à p_j-w ou bien encore à

$w' \equiv w \times z \pmod{p_j}$ ou bien à $p_j - w'$.

Pour $p_j \equiv 2^t+1 \pmod{2^{t+1}}$ avec $t > 2$, la clé $\langle (p_j-1+2^t)/2^{t+1}, p_j \rangle$ donne la racine carrée de rang impair de n'importe quel élément de rang impair. Le test de compatibilité entre k, g et p a donné la valeur de h, puis celle de u.

- Lorsque G_i est dans un cycle ($u = 0$, quelle que soit la valeur de k), on établit un nombre $s_j \equiv ((p_j-1+2^t)/2^{t+1})^k \pmod{(p_j-1)/2^t}$. La clé $\langle s_j, p_j \rangle$ transforme G_i en la solution de rang impair $w \equiv G_i^{s_j} \pmod{p_j}$. Il y des solutions de rang pair réparties dans $\min(k, t)$ branches consécutives rattachées au cycle, disons dans α branches. $Q_{i,j}$ est égal au produit de w par n'importe laquelle des racines 2^α-ièmes de l'unité dans $CG(p_j)$.
- Lorsque G_i est en position appropriée dans une branche ($u > 0$, $u+k \leq t$), toutes les solutions sont dans la même branche que G_i, branche rattachée à un cycle par la puissance 2^u-ième du nombre G_i. On établit un nombre $s_j \equiv ((p_j-1+2^t)/2^{t+1})^{k+u} \pmod{(p_j-1)/2^t}$. La clé $\langle s_j, p_j \rangle$ transforme la puissance 2^u-ième de G_i en un nombre de rang impair w. L'ensemble des produits de w par les racines 2^{k+u}-ièmes primitives de l'unité dans $CG(p_j)$ comprend les 2^k valeurs de $Q_{i,j}$.

Lorsque p_j est tel que $t \geq k$, le nombre b_j étant une racine 2^t-ième primitive de l'unité dans $CG(p_j)$, la puissance 2^{t-u}-ième de b_j dans $CG(p_j)$ existe ; c'est une racine 2^k-ième primitive de l'unité. Multiplier $Q_{i,j}$ par une racine 2^k-ième primitive de l'unité permet de basculer la valeur du nombre $\Delta_{i,j}$.

Pour une équation de type inverse : $1 \equiv x^v \times g_i^2 \pmod{p_j}$, il suffit de remplacer le nombre s_j par $((p_j-1)/2^t)-s_j$ dans la clé $\langle s_j, p_j \rangle$, ce qui revient à inverser la valeur de $Q_{i,j}$ dans $CG(p_j)$.

Exemple de jeu de clés à deux facteurs premiers congrus à 5 (mod 8)

p_1 = E6C83BF428689AF8C35E07EDD06F9B39A659829A58B79CD894C
435C95F32BF25

p_2 = 11BF8A68A0817BFCC00F15731C8B70CEF9204A34133A0DEF862
829B2EEA74873D

$n = p_1 \times p_2$ = FFFF8263434F173D0F2E76B32D904F56F4A5A6A50008C43
D32B650E9AB9AAD2EB713CD4F9A97C4DBDA3828A3954F296458D5
F42C0126F5BD6B05478BE0A80ED1

Voici les symboles de Legendre des tout premiers nombres premiers.

$(2 \mid p_1) = -1$; $(3 \mid p_1) = -1$; $(5 \mid p_1) = +1$; $(7 \mid p_1) = -1$;
$(11 \mid p_1) = +1$; $(13 \mid p_1) = -1$; $(17 \mid p_1) = +1$;

Dans CG(p_1), le rang est impair pour -5, -11 et 17.

$(2 \mid p_2) = -1$; $(3 \mid p_2) = +1$; $(5 \mid p_2) = +1$; $(7 \mid p_2) = +1$;
$(11 \mid p_2) = +1$; $(13 \mid p_2) = -1$; $(17 \mid p_2) = -1$;

Dans CG(p_2), le rang est impair pour 3, -5, 7 et 11.

La fonction de Carmichael est $\lambda(n) = \text{ppcm}((p_1-1)/4, (p_2-1)/4)$.

$\lambda(n)$ = 33331A13DA4304A5CFD617BD6F83431164212154334F40C3D5
7A9C8558555D5BDAA2EF6AED17B9E3794F51A65A1B37239B18FA9
B0F618627D8C7E1D8499C1B

Avec $k = 9$, on utilise le nombre $\sigma \equiv \lambda(n) - ((1+\lambda(n))/2)^9 \pmod{\lambda(n)}$ comme exposant privé, de façon à utiliser des équations génériques de type inverse.

σ = 01E66577BC997CAC273671E187A35EFD25373ABC9FE6770E7446
C0CCEF2C72AF6E89D0BE277CC6165F1007187AC58028BD2416D4CC
1121E7A7A8B6AE186BB4B0

Les nombres 2, 3, 7, 13 et 17 ne conviennent pas comme nombre de base.

La clé $\langle \sigma, n \rangle$ transforme $g_1 = 5$ en un nombre privé Q_1 qui ne révèle pas de décomposition. En effet, dans les deux corps, -5 est sur un cycle.

Q_1 = 818C23AF3DE333FAECE88A71C4591A70553F91D6C0DD5538EC
0F2AAF909B5BDAD491FD8BF13F18E3DA3774CCE19D0097BC4BD4
7C5D6E0E7EBF6D89FE3DC5176C

La clé $\langle \sigma, n \rangle$ transforme $g_2 = 11$ en un nombre privé Q_2 qui révèle une décomposition. En effet, 11 n'est pas en même position dans les deux corps.

Q_2 = 25F9AFDF177993BE8652CE6E2C728AF31B6D66154D3935AC535
196B07C19080DC962E4E86ACF40D01FDC454F2565454F290050DA05

2089EEC96A1B7DEB92CCA7

La clé $\langle \sigma, n \rangle$ transforme $g_3 = 21 = 3 \times 7$ en un nombre privé Q_3 qui révèle une décomposition.

Q_3 = 78A8A2F30FEB4A5233BC05541AF7B684C2406415EA1DD67D18 A0459A1254121E95D5CAD8A1FE3ECFE0685C96CC7EE86167D99532 B3A96B6BF9D93CAF8D4F6AF0

La clé $\langle \sigma, n \rangle$ transforme $g_4 = 26 = 2 \times 13$ en un nombre privé Q_4 qui révèle une décomposition.

Q_4 = 6F1748A6280A200C38824CA34C939F97DD2941DAD300030E481 B738C62BF8C673731514D1978AF5655FE493D659514A6CE897AB76C 01E50B5488C5DAD12332E5

La clé privée peut encore se représenter par les deux facteurs premiers, le paramètre des restes chinois et huit composantes privées.

$\alpha \equiv (p_2 \pmod{p_1})^{-1} \pmod{p_1}$ = ADE4E77B703F5FDEAC5B9AAE825D649 E06692D15FBF0DF737B115DC4D012FD1D

$Q_{1,1} \equiv Q_1 \pmod{p_1}$ = 7751A9EE18A8F5CE44AD73D613A4F465E06C6F9 AF4D229949C74DD6C18D76FAF

$Q_{1,2} \equiv Q_1 \pmod{p_2}$ = A9EB5FA1B2A981AA64CF88C382923DB64376F5F D48152C08EEB6114F31B7665F

$Q_{2,1} \equiv Q_2 \pmod{p_1}$ = D5A7D33C5FB75A033F2F0E8B20274B957FA3400 4ABB2C2AC1CA3F5320C5A9049

$Q_{2,2} \equiv Q_2 \pmod{p_2}$ = 76C9F5EFD066C73A2B5CE9758DB512DFC011F5B 5AF7DA8D39A961CC876F2DD8F

$Q_{3,1} \equiv Q_3 \pmod{p_1}$ = 2FEC0DC2DCA5BA7290B27BC8CC85C938A514B 8F5CFD55820A174FB5E6DF7B883

$Q_{3,2} \equiv Q_3 \pmod{p_2}$ = 010D488E6B0A38A1CC406CEE0D55DE59013389D 8549DE493413F34604A160C1369

$Q_{4,1} \equiv Q_4 \pmod{p_1}$ = A2B32026B6F82B6959566FADD9517DB8ED85246 52145EE159DF3DC0C61FE3617

$Q_{4,2} \equiv Q_4 \pmod{p_2}$ = 011A3BB9B607F0BD71BBE25F52B305C224899E5
F1F8CDC2FE0D8F9FF62B3C9860F

Polymorphisme de la clé privée GQ2 — Les diverses représentations possibles de la clé privée GQ2 s'avèrent équivalentes : elles se ramènent toutes à la connaissance de la factorisation du module n qui est la véritable clé privée GQ2. La représentation de la clé privée GQ2 a un effet sur le déroulement des calculs au sein de l'entité qui prouve, pas au sein de l'entité qui contrôle. Voici les trois principales représentations possibles de la clé privée GQ2. 1) La représentation classique des clés privées GQ consiste à stocker m nombres privés Q_i et la clé publique de vérification $\langle v, n \rangle$; pour les schémas GQ2, cette représentation est concurrencée par les deux suivantes. 2) La représentation optimale en termes de charges de travail consiste à stocker le paramètre k, les f facteurs premiers p_j, $m \times f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois. 3) La représentation optimale en termes de taille de clé privée consiste à stocker le paramètre k, les m nombres de base g_i et les f facteurs premiers p_j, puis, à commencer chaque utilisation en établissant ou bien m nombres privés Q_i et le module n pour se ramener à la première représentation, ou bien $m \times f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois pour se ramener à la seconde.

Parce que la sécurité du mécanisme d'authentification dynamique ou de signature numérique équivaut à la connaissance d'une décomposition du module, les schémas GQ2 ne permettent pas de distinguer simplement deux entités utilisant le même module. Généralement, chaque entité qui prouve dispose de son propre module GQ2. Toutefois, on peut spécifier des modules GQ2 à quatre facteurs premiers dont deux sont connus d'une entité et les deux autres d'une autre.

Authentification dynamique — Le mécanisme d'authentification dynamique est destiné à prouver à une entité appelée **contrôleur** l'authenticité

d'une autre entité appelée **démonstrateur** ainsi que l'authenticité d'un éventuel message associé M, de sorte que le contrôleur s'assure qu'il s'agit bien du démonstrateur et éventuellement que lui et le démonstrateur parlent bien du même message M. Le message associé M est optionnel, ce qui signifie qu'il peut être vide.

Le mécanisme d'authentification dynamique est une séquence de quatre actes : un acte d'engagement, un acte de défi, un acte de réponse et un acte de contrôle. Le démonstrateur joue les actes d'engagement et de réponse. Le contrôleur joue les actes de défi et de contrôle.

Au sein du démonstrateur, on peut isoler un témoin, de manière à isoler les paramètres et les fonctions les plus sensibles du démonstrateur, c'est-à-dire, la production des engagements et des réponses. Le témoin dispose du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus : • les f facteurs premiers et les m nombres de base, • les $m \times f$ composantes privées, les f facteurs premiers et $f-1$ paramètres des restes chinois, • les m nombres privés et le module n.

Le témoin peut correspondre à une réalisation particulière, par exemple, • une carte à puce reliée à un PC formant ensemble le démonstrateur, ou encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce. Le témoin ainsi isolé est semblable au témoin défini ci-après au sein du signataire. A chaque exécution du mécanisme, le témoin produit un ou plusieurs engagements R, puis, autant de réponses D à autant de défis d. Chaque ensemble $\{R, d, D\}$ constitue un **triplet GQ2**.

Outre qu'il comprend le témoin, le démonstrateur dispose également, le cas échéant, d'une fonction de hachage et d'un message M.

Le contrôleur dispose du module n, par exemple, à partir d'un annuaire de clés publiques ou encore à partir d'un certificat de clés publique ; le cas

échéant, il dispose également de la même fonction de hachage et d'un message M'. Les paramètres publics GQ2, à savoir les nombres k, m et g_1 à g_m peuvent être donnés au contrôleur par le démonstrateur. Le contrôleur est apte à reconstituer un engagement R' à partir de n'importe quel défi d et de n'importe quelle réponse D. Les paramètres k et m renseignent le contrôleur. Faute d'indication contraire, les m nombres de base de g_1 à g_m sont les m premiers nombres premiers. Chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m : un par nombre de base. Chaque défi élémentaire de d_1 à d_m est un nombre de 0 à $2^{k-1}-1$ (les nombres de $v/2$ à $v-1$ ne sont pas utilisés). Typiquement, chaque défi est codé par m fois $k-1$ bits (et non pas m fois k bits). Par exemple, avec $k = 5$ et $m = 4$ nombres de base 5, 11, 21 et 26, chaque défi comporte 16 bits transmis sur quatre quartets. Lorsque les $(k-1)\times m$ défis possibles sont également probables, le nombre $(k-1)\times m$ détermine la sécurité apportée par chaque triplet GQ2 : un imposteur qui, par définition, ne connaît pas la factorisation du module n a exactement une chance de succès sur $2^{(k-1)\times m}$. Lorsque $(k-1)\times m$ vaut de 15 à 20, un triplet suffit à assurer raisonnablement l'authentification dynamique. Pour atteindre n'importe quel niveau de sécurité, on peut produire des triplets en parallèle ; on peut également en produire en séquence, c'est-à-dire, répéter l'exécution du mécanisme.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin n'utilise pas les restes chinois, il dispose du paramètre k, des m nombres privés de Q_1 à Q_m et du module n ; il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Voici un exemple avec le jeu de clés précédent sans les restes chinois.

r = 5E94B894AC24AF843131F437C1B1797EF562CFA53AB8AD426C1
AC016F1C89CFDA13120719477C3E2FB4B4566088E10EF9C010E8F09

C60D981512198126091996

R = 6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E330
0EBF234FA0BC20A95152A8FB73DE81FAEE5BF4FD3EB7F5EE3E36D
7068D083EF7C93F6FDDF673A

Lorsque le témoin utilise les restes chinois, il dispose du paramètre k, des f facteurs premiers de p_1 à p_f, de f–1 paramètres des restes chinois et des $m \times f$ composantes privées $Q_{i,j}$; il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i), il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

$$R = \text{Restes Chinois}(R_1, R_2, \ldots R_f)$$

Voici un exemple avec le jeu de clés précédent et avec les restes chinois.

r_1 = 5C6D37F0E97083C8D120719475E080BBBF9F7392F11F3E244FDF0
204E84D8CAE

R_1 = 3DDF516EE3945CB86D20D9C49E0DA4D42281D07A76074DD4FE
C5C7C5E205DF66

r_2 = AC8F85034AC78112071947C457225E908E83A2621B0154ED15DB
FCB9A4915AC3

R_2 = 01168CEC0F661EAA15157C2C287C6A5B34EE28F8EB4D8D34085
8079BCAE4ECB016

R = Restes Chinois(R_1, R_2) = 0AE51D90CB4FDC3DC757C56E063C9ED8
6BE153B71FC65F47C123C27F082BC3DD15273D4A923804718573F2F0
5E991487D17DAE0AAB7DF0D0FFA23E0FE59F95F0

Dans les deux cas, le démonstrateur transmet au contrôleur tout ou partie de chaque engagement $\boldsymbol{R}$, ou bien, un code de hachage $\boldsymbol{H}$ obtenu en hachant

chaque engagement ***R*** et un message ***M***.

2) L'acte de défi consiste à tirer au hasard un ou plusieurs défis d composés chacun de m défis élémentaires $d_1 \quad d_2 \ \ldots \ d_m$; chaque défi élémentaire d_i est l'un des nombres de 0 à $v/2-1$.

$$d = d_1 \ d_2 \ \ldots \ d_m$$

Voici un défi pour les deux exemples, c'est-à-dire avec $k = 5$ et $m = 4$.

$$d_1 = 1011 = 11 = \text{'B'} \ ; \ d_2 = 0011 = 3 \ ; \ d_3 = 0110 = 6 \ ; \ d_4 = 1001 = 9,$$

$$d = d_1 \ || \ d_2 \ || \ d_3 \ || \ d_4 = 10110011 \ 01101001 = \text{B3 69}$$

Le contrôleur transmet au démonstrateur chaque défi ***d***.

3) L'acte de réponse comporte les opérations suivantes.

Lorsque le témoin n'utilise pas les restes chinois, il dispose du paramètre k, des m nombres privés de Q_1 à Q_m et du module n ; il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les nombres privés selon les défis élémentaires.

$$D \equiv r \times Q_1^{d_1} \times Q_2^{d_2} \times \ldots Q_m^{d_m} \pmod{n}$$

Voici la suite de l'exemple sans les restes chinois.

D = 027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A7870E6C1940F7A6996C2D871EBE611812532AC5875E0E116CC8BA648FD8E86BE0B2ABCC3CCBBBE4

Lorsque le témoin utilise les restes chinois, il dispose du paramètre k, des f facteurs premiers de p_1 à p_f, de $f-1$ paramètres des restes chinois et des $m \times f$ composantes privées $Q_{i,j}$; il calcule une ou plusieurs collections de f composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$D_i \equiv r_i \times Q_{1,i}^{d_1} \times Q_{2,i}^{d_2} \times \ldots Q_{m,i}^{d_m} \pmod{p_i}$$

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

Voici la suite de l'exemple avec les restes chinois.

$D_1 = r_1 \times Q_{1,1}^{d1} \times Q_{2,1}^{d2} \times Q_{3,1}^{d3} \times Q_{4,1}^{d4} \pmod{p_1} =$
C71F86F6FD8F955E2EE434BFA7706E38E5E715375BC2CD2029A4BD
572A9EDEE6

$D_2 = r_2 \times Q_{1,2}^{d1} \times Q_{2,2}^{d2} \times Q_{3,2}^{d3} \times Q_{4,2}^{d4} \pmod{p_2} =$
0BE022F4A20523F98E9F5DBEC0E10887902F3AA48C864A6C354693A
D0B59D85E

$D =$ 90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98
C8577A660B9CFCEAECB93BE1BCC356811BF12DD667E2270134C907
3B9418CA5EBF5191218D3FDB3

Dans les deux cas, le démonstrateur transmet chaque réponse ***D*** au contrôleur.

4) L'acte de contrôle consiste à contrôler que chaque triplet $\{R, d, D\}$ vérifie une équation du type suivant pour une valeur non nulle,

$$R \times \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

ou bien, à rétablir chaque engagement : aucun ne doit être nul.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Eventuellement, le contrôleur calcule ensuite un code de hachage H' en hachant chaque engagement rétabli R' et un message M'. L'authentification dynamique est réussie lorsque le contrôleur retrouve ainsi ce qu'il a reçu à l'issue de l'acte d'engagement, c'est-à-dire, tout ou partie de chaque engagement R, ou bien, le code de hachage H.

Par exemple, une séquence d'opérations élémentaires transforme la réponse D en un engagement R'. La séquence comprend k carrés (mod n) séparés par k–1 divisions ou multiplications (mod n) par des nombres de base. Pour la i ième division ou multiplication, qui s'effectue entre le i ième carré et le

i+1 ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, ... jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m.

Voici la fin de l'exemple sans les restes chinois.

D = 027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A787
0E6C1940F7A6996C2D871EBE611812532AC5875E0E116CC8BA648FD
8E86BE0B2ABCC3CCBBBE4

Elever au carré modulo n :

88BA681DD641D37D7A7D9818D0DBEA82174073997C6C32F7FCAB3
0380C4C6229B0706D1AF6EBD84617771C31B4243C2F0376CAF5DCE
B644F098FAF3B1EB49B39

Multiplier par 5 fois 26 = 130, soit '82' modulo n :

6ECABA65A91C22431C413E4EC7C7B39FDE14C9782C94FD6FA3CA
AD7AFE192B9440C1113CB8DBC45619595D263C1067D3D0A840FDE0
08B415028AB3520A6AD49D

Elever au carré modulo n :

0236D25049A5217B13818B39AFB009E4D7D52B17486EBF844D64CF7
5C4F652031041328B29EBF0829D54E3BD17DAD218174A01E6E3AA65
0C6FD62CC274426607

Multiplier par 21, soit '15' modulo n :

2E7F40960A8BBF1899A06BBB6970CFC5B47C88E8F115B5DA594504
A92834BA405559256A705ABAB6E7F6AE82F4F33BF9E91227F0ACFA
4A052C91ABF389725E93

Elever au carré modulo n :

B802171179648AD687E672D3A32640E2493BA2E82D5DC87DBA2B2C
C0325E7A71C50E8AE02E299EF868DD3FB916EBCBC0C5569B53D42
DAD49C956D8572E1285B0

Multiplier par 5 fois 11 fois 21 = 1155, soit '483' modulo n :

3305560276310DEFEC1337EB5BB5810336FDB28E91B350D485B09188

E0C4F1D67E68E9590DB7F9F39C22BDB4533013625011248A8DC417C
667B419D27CB11F72

Elever au carré modulo n :

8871C494081ABD1AEB8656C38B9BAAB57DBA72A4BD4EF9029ECB
FFF540E55138C9F22923963151FD0753145DF70CE22E9D019990E41D
B6104005EEB7B1170559

Multiplier par 5 fois 11 fois 26 = 1430, soit '596' modulo n :

2CF5F76EEBF128A0701B56F837FF68F81A6A5D175D0AD67A14DAE
C6FB68C362B1DC0ADD6CFC004FF5EEACDF794563BB09A17045EC
FFF88F5136C7FBC825BC50C

Elever au carré modulo n :

6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E3300EB
F234FA0BC20A95152A8FB73DE81FAEE5BF4FD3EB7F5EE3E36D706
8D083EF7C93F6FDDF673A

On retrouve bien l'engagement $\boldsymbol{R}$. L'authentification est réussie.

Voici la fin de l'exemple avec les restes chinois.

D = 90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98
C8577A660B9CFCEAECB93BE1BCC356811BF12DD667E2270134C907
3B9418CA5EBF5191218D3FDB3

Elever au carré modulo n :

770192532E9CED554A8690B88F16D013010C903172B266C1133B136E
BE3EB5F13B170DD41F4ABE14736ADD3A70DFA43121B6FC5560CD
D4B4845395763C792A68

Multiplier par 5 fois 26 = 130, soit '82' modulo n :

6EE9BEF9E52713004971ABB9FBC31145318E2A703C8A2FB3E144E77
86397CD8D1910E70FA86262DB771AD1565303AD6E4CC6E90AE3646
B461D3521420E240FD4

Elever au carré modulo n :

D9840D9A8E80002C4D0329FF97D7AD163D8FA98F6AF8FE2B2160B2

126CBBDFC734E39F2C9A39983A426486BC477F20ED2CA59E664C23
CA0E04E84F2F0AD65340

Multiplier par 21, soit '15' modulo n :

D7DD7516383F78944F2C90116E1BEE0CCDC8D7CEC5D7D1795ED33
BFE8623DB3D2E5B6C5F62A56A2DF4845A94F32BF3CAC360C7782B
5941924BB4BE91F86BD85F

Elever au carré modulo n :

DD34020DD0804C0757F29A0CBBD7B46A1BAF949214F74FDFE021B
626ADAFBAB5C3F1602095DA39D70270938AE362F2DAE0B91485531
0C7BCA328A4B2643DCCDF

Multiplier par 5 fois 11 fois 21 = 1155, soit '483' modulo n :

038EF55B4C826D189C6A48EFDD9DADBD2B63A7D675A0587C85596
18EA2D83DF552D24EAF6BE983FB4AFB3DE7D4D2545190F1B1F946
D327A4E9CA258C73A98F57

Elever au carré modulo n :

D1232F50E30BC6B7365CC2712E5CAE079E47B971DA03185B33E918E
E6E99252DB3573CC87C604B327E5B20C7AB920FDF142A8909DBBA1
C04A6227FF18241C9FE

Multiplier par 5 fois 11 fois 26 = 1430, soit '596' modulo n :

3CC768F12AEDFCD4662892B9174A21D1F0DD9127A54AB63C984019
BED9BF88247EF4CCB56D71E0FA30CFB0FF28B7CE45556F744C1FD7
51BFBCA040DC9CBAB744

Elever au carré modulo n :

0AE51D90CB4FDC3DC757C56E063C9ED86BE153B71FC65F47C123C
27F082BC3DD15273D4A923804718573F2F05E991487D17DAE0AAB7
DF0D0FFA23E0FE59F95F0

On retrouve bien l'engagement R. L'authentification est réussie.

Signature numérique

Le mécanisme de signature numérique permet à une entité appelée

signataire de produire des messages signés et à une entité appelée **contrôleur** de vérifier des messages signés. Le message M est une séquence binaire quelconque : il peut être vide. Le message M est signé en lui adjoignant un appendice de signature qui comprend un ou plusieurs engagements et / ou défis, ainsi que les réponses correspondantes.

Le contrôleur dispose du module n, par exemple, à partir d'un annuaire de clés publiques ou encore à partir d'un certificat de clés publique ; il dispose également de la même fonction de hachage. Les paramètres publics GQ2, à savoir les nombres k, m et g_1 à g_m peuvent être donnés au contrôleur par le démonstrateur, par exemple, en les mettant dans l'appendice de signature.

Les nombres $\boldsymbol{k}$ et $\boldsymbol{m}$ renseignent le contrôleur. D'une part, chaque défi élémentaire, de d_1 à d_m, est un nombre de 0 à $2^{k-1}-1$ (les nombres $v/2$ à $v-1$ ne sont pas utilisés). D'autre part, chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m, autant que de nombres de base. En outre, faute d'indication contraire, les m nombres de base, de g_1 à g_m, sont les m premiers nombres premiers. Avec $(k-1)\times m$ valant de 15 à 20, on peut signer avec quatre triplets GQ2 produits en parallèle ; avec $(k-1)\times m$ valant 60 ou plus, on peut signer avec un seul triplet GQ2. Par exemple, avec $k = 9$ et $m = 8$, un seul triplet GQ2 suffit ; chaque défi comporte huit octets et les nombres de base sont 2, 3, 5, 7, 11, 13, 17 et 19.

L'opération de signature est une séquence de trois actes : un acte d'engagement, un acte de défi et un acte de réponse. Chaque acte produit un ou plusieurs triplets GQ2 comprenant chacun : un engagement R ($\neq 0$), un défi d composé de m défis élémentaires notés par d_1, d_2, ... d_m et une réponse D ($\neq 0$).

Le signataire dispose d'une fonction de hachage, du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. **Au sein du signataire, on peut isoler un témoin qui exécute les actes d'engagement et de réponse**, de

manière à isoler les fonctions et les paramètres les plus sensibles du démonstrateur. Pour calculer engagements et réponses, le témoin dispose du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. Le témoin ainsi isolé est semblable au témoin défini au sein du démonstrateur. Il peut correspondre à une réalisation particulière, par exemple, • une carte à puce reliée à un PC formant ensemble le signataire, ou encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin dispose des m nombres privés Q_1 à Q_m et du module n, il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m \times f$ composantes privées $Q_{i,j}$, il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i), il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

$$R = \text{Restes Chinois}(R_1, R_2, \ldots R_f)$$

2) L'acte de défi consiste à hacher tous les engagements R et le message à signer M pour obtenir un code de hachage à partir duquel le signataire forme un ou plusieurs défis comprenant chacun m défis élémentaires ; chaque défi élémentaire est un nombre de 0 à $v/2-1$; par exemple, avec

$k = 9$ et $m = 8$, chaque défi comporte huit octets. Il y a autant de défis que d'engagements.

$$d = d_1\ d_2 \ldots\ d_m, \text{ extraits du résultat Hash}(M, R)$$

3) L'acte de réponse comporte les opérations suivantes.

Lorsque la témoin dispose des m nombres privés Q_1 à Q_m et du module n, il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les nombres privés selon les défis élémentaires.

$$X \equiv Q_1^{d_1} \times Q_2^{d_2} \times \ldots Q_m^{d_m} \pmod{n}$$

$$D \equiv r \times X \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m \times f$ composantes privées $Q_{i,j}$, il calcule une ou plusieurs collections de f composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$X_i \equiv Q_{1,i}^{d_1} \times Q_{2,i}^{d_2} \times \ldots Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i \times X_i \pmod{p_i}$$

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

Le signataire signe le message M en lui adjoignant un appendice de signature comprenant :

- ou bien, chaque triplet GQ2, c'est-à-dire, chaque engagement R, chaque défi d et chaque réponse D,
- ou bien, chaque engagement R et chaque réponse D correspondante,
- ou bien, chaque défi d et chaque réponse D correspondante.

Le déroulement de l'opération de vérification dépend du contenu de l'appendice de signature. On distingue les trois cas.

Au cas où l'appendice comprend un ou plusieurs triplets, l'opération de

contrôle comporte deux processus indépendants dont la chronologie est indifférente. Le contrôleur accepte le message signé si et seulement si les deux conditions suivantes sont remplies.

D'une part, chaque triplet doit être cohérent (une relation appropriée du type suivant doit être vérifiée) et recevable (la comparaison doit se faire sur une valeur non nulle).

$$R \times \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Par exemple, on transforme la réponse D par une séquence d'opérations élémentaires : k carrés (mod n) séparés par k–1 multiplications ou divisions (mod n) par des nombres de base. Pour la i ième multiplication ou division, qui s'effectue entre le i ième carré et le i+1 ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, … jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m. On doit ainsi retrouver chaque engagement R présent dans l'appendice de signature.

D'autre part, le ou les triplets doivent être liés au message M. En hachant tous les engagements R et le message M, on obtient un code de hachage à partir duquel on doit retrouver chaque défi d.

$d = d_1\ d_2 \ldots\ d_m$, identiques à ceux extraits du résultat Hash(M, R)

Au cas où l'appendice ne comprend pas de défi, l'opération de contrôle commence par la reconstitution de un ou plusieurs défis d' en hachant tous les engagements R et le message M.

$d' = d'_1\ d'_2 \ldots\ d'_m$, extraits du résultat Hash(M, R)

Ensuite, le contrôleur accepte le message signé si et seulement si chaque triplet est cohérent (une relation appropriée du type suivant est vérifiée) et recevable (la comparaison se fait sur une valeur non nulle).

$$R \times \prod_{i=1}^{m} G_i^{d'_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d'_i} \pmod{n}$$

Au cas où l'appendice ne comprend pas d'engagement, l'opération de contrôle commence par la reconstitution de un ou plusieurs engagements R' selon une des deux formules suivantes, celle qui est appropriée. Aucun engagement rétabli ne doit être nul.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Ensuite, le contrôleur doit hacher tous les engagements R' et le message M de façon à reconstituer chaque défis d.

$d = d_1\ d_2 \ldots\ d_m$, identiques à ceux extraits du résultat Hash(M, R')

Le contrôleur accepte le message signé si et seulement si chaque défi reconstitué est identique au défi correspondant figurant en appendice.

ANNEXE 1

Procédé, système, dispositif destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message aux moyens de facteurs premiers particuliers.

La présente invention concerne le domaine technique des procédés, des systèmes ainsi que des dispositifs destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Le brevet EP 0 311 470 B1 dont les inventeurs sont Louis Guillou et Jean-Jacques Quisquater décrit un tel procédé. On y fera ci-après référence en le désignant par les termes : "brevet GQ" ou "procédé GQ". Par la suite on désignera parfois par "GQ2", "invention GQ2" ou "technologie GQ2" de nouveaux développements de la technologie GQ faisant l'objet des demandes pendantes déposées le même jour que la présente demande par France Télécom, TDF et la Société Mathrizk et ayant pour inventeur Louis Guillou et Jean-Jacques Quisquater. Les traits caractéristiques de ces demandes pendantes sont rappelés chaque fois que cela est nécessaire dans la description qui suit.

Selon le procédé GQ, une entité appelée " autorité de confiance " attribue une identité à chaque entité appelée " témoin " et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : " *Voici mon identité ; j'en connais la signature RSA.* " Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée " contrôleur " vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant le procédé GQ se déroulent " sans transfert de connaissance ". Selon le procédé GQ, le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

La technologie GQ précédemment décrite fait appel à la technologie RSA. Mais si la technologie RSA dépend bel et bien de la factorisation du module n, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites "multiplicatives" contre les diverses normes de signature numérique mettant en oeuvre la technologie RSA.

L'objectif de la technologie GQ2 est double : d'une part, améliorer les performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La connaissance de la clé privée GQ2 est équivalente à la connaissance de la factorisation du module n. Toute attaque au niveau des triplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 évite les inconvénients présentés par la technologie RSA.

Le procédé GQ met en œuvre des calculs modulo des nombres de 512 bits ou davantage. Ces calculs concernent des nombres ayant sensiblement la même taille élevés à des puissances de l'ordre de $2^{16} + 1$. Or les infrastructures microélectroniques existantes, notamment dans le domaine des cartes bancaires, font usage de microprocesseurs auto-programmables monolithiques dépourvus de coprocesseurs arithmétiques. La charge de travail liée aux multiples opérations arithmétiques impliquées par des procédés tels que le procédé GQ, entraîne des temps de calcul qui dans certains cas s'avèrent pénalisant pour les consommateurs utilisant des cartes bancaires pour acquitter leurs achats. Il est rappelé ici, qu'en cherchant à accroître la sécurité des cartes de paiement, les autorités bancaires posent un problème particulièrement délicat à résoudre. En effet, il faut traiter deux questions apparemment contradictoires : augmenter la

sécurité en utilisant des clés de plus en plus longues et distinctes pour chaque carte tout en évitant que la charge de travail n'entraîne des temps de calcul prohibitifs pour les utilisateurs. Ce problème prend un relief particulier dans la mesure où, en outre, il convient de tenir compte de l'infrastructure en place et des composants microprocesseurs existants.

La technologie GQ2 apporte une solution à ce problème tout en renforçant la sécurité.

La technologie GQ2 met en oeuvre des facteurs premiers ayant des propriétés particulières. Différentes techniques existent pour produire ces facteurs premiers. La présente invention a pour objet un procédé permettant de produire de manière systématique de tels facteurs premiers. Elle concerne aussi l'application qui peut être faite de ceux-ci plus particulièrement dans la mise en oeuvre de la technologie GQ2. On souligne dès à présent que ces facteurs premiers particuliers et le procédé permettant de les obtenir sont susceptibles d'application en dehors du champ de la technologie GQ2.

L'invention s'applique à un procédé (procédé GQ2) destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- un module public **n** constitué par le produit de **f** facteurs premiers $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** ;
- **m** nombres de base $\mathbf{g_1}$, $\mathbf{g_2}$, ... $\mathbf{g_m}$ entiers, distincts, (**m** étant supérieur ou égal à 1).

Les nombres de base $\mathbf{g_i}$ sont tels que les deux équations (1) et (2) :

$$\mathbf{x^2 \equiv g_i \bmod n} \quad \text{et} \quad \mathbf{x^2 \equiv - g_i \bmod n}$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n**,
et tel que l'équation (3):

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

Le procédé selon l'invention permet de produire les **f** facteurs premiers p_1, p_2, ... p_f de telle sorte que les équations (1), (2) et (3) soient satisfaites. Le procédé selon l'invention comprend l'étape de choisir en premier :

- les **m** nombres de base g_1, g_2, ... g_m,
- la taille du module **n**,
- la taille des **f** facteurs premiers p_1, p_2, ... p_f.

Le procédé concerne le cas où l'exposant public **v** est de la forme :

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1. On choisit également en premier le paramètre de sécurité **k**. Cette valeur particulière de l'exposant **v** est un des traits essentiels de la technologie GQ2.

De préférence, les **m** nombres de base g_1, g_2, ... g_m, sont choisis au moins en partie parmi les premiers nombres entiers. De préférence également, le paramètre de sécurité **k** est un petit nombre entier, notamment inférieur à 100. Avantageusement, la taille du module **n** est supérieure à plusieurs centaines de bits. Avantageusement également, les **f** facteurs premiers p_1, p_2, ... p_f ont une taille voisine de la taille du module **n** divisé par le nombre **f** de facteurs.

Selon une caractéristique importante du procédé selon l'invention, les **f** facteurs premiers p_1, p_2, ... p_f ne sont pas choisis de manière quelconque. Parmi les **f** facteurs premiers p_1, p_2, ... p_f un certain nombre d'entre eux : **e** seront choisis congrus à 1 modulo 4. Ce nombre **e** de facteurs premiers peut être nul. Dans le cas où **e** est nul le module **n** sera ci-après qualifié de module basique, dans le cas où $e > 0$ le module **n** sera ci-après qualifié de module mixte. Les **f-e** autres facteurs premiers sont choisis congrus à 3

modulo 4. Ce nombre **f-e** de facteurs premiers est au moins égal à 2.

Choix des f-e facteurs premiers congrus à 3 modulo 4

Pour produire les **f-e** facteurs premiers $\mathbf{p}_1$, $\mathbf{p}_2$, ... $\mathbf{p}_{f-e}$ congrus à 3 modulo 4, on met en oeuvre les étapes suivantes :

- on choisit le premier facteur premier $\mathbf{p}_1$ congru à 3 modulo 4 puis,

- on choisit le deuxième facteur premier $\mathbf{p}_2$ tel que $\mathbf{p}_2$ soit complémentaire de $\mathbf{p}_1$ par rapport au nombre de base $\mathbf{g}_1$.

Pour choisir le facteur $\mathbf{p}_{i+1}$, on procède comme suit en distinguant deux cas:

(1) Cas où i> m

Dans le cas où i> m, on choisit le facteur $\mathbf{p}_{i+1}$ congru à 3 modulo 4.

(2) Cas où i≤ m

Dans ce cas où i≤ m, on calcule le profil ($\mathbf{Profil}_i(\mathbf{g}_i)$) de $\mathbf{g}_i$ par rapport aux i premiers facteurs premiers $\mathbf{p}_i$,

• si le $\mathbf{Profil}_i(\mathbf{g}_i)$ est plat, on choisit le facteur $\mathbf{p}_{i+1}$ tel que $\mathbf{p}_{i+1}$ soit complémentaire de $\mathbf{p}_1$ par rapport à $\mathbf{g}_i$,

• sinon, on choisit parmi les **i-1** nombres de bases $\mathbf{g}_1$, $\mathbf{g}_2$, ... $\mathbf{g}_{i-1}$ et toutes leurs combinaisons multiplicatives le nombre, ci-après dénommé **g**, tel que $\mathbf{Profil}_i(\mathbf{g}) = \mathbf{Profil}_i(\mathbf{g}_i)$, on choisit ensuite $\mathbf{p}_{i+1}$ tel que $\mathbf{Profil}_{i+1}(\mathbf{g}_i) \neq \mathbf{Profil}_{i+1}(\mathbf{g})$.

Les expressions "complémentaire", "profil", "profil plat" ont le sens défini dans la description.

Pour choisir le dernier facteur premier $\mathbf{p}_{f-e}$ on procède comme suit, en distinguant trois cas :

(1) Cas où f-e-1 > m

Dans le cas où f-e-1 > m, on choisit $\mathbf{p}_{f-e}$ congru à 3 modulo 4.

(2) Cas où f-e-1 = m

Dans le cas où f-e-1 = m, on calcule $\mathbf{Profil}_{f-e-1}(\mathbf{g}_m)$ par rapport aux f-e-1 premiers facteurs premiers, de $\mathbf{p}_1$ à $\mathbf{p}_{f-e-1}$,

• si $\mathbf{Profil_{f\text{-}e\text{-}1}(g_m)}$ est plat, on choisit $\mathbf{p_{f\text{-}e\text{-}1}}$ tel qu'il soit complémentaire de $\mathbf{p_1}$ par rapport à $\mathbf{g_m}$,

• sinon, on procède comme il est ci-après stipulé.

On choisit parmi les **m-1** nombres de bases de $\mathbf{g_1}$ à $\mathbf{g_{m-1}}$ et toutes leurs combinaisons multiplicatives le nombre, ci-après dénommé **g,** tel que $\mathbf{Profil_i(g) = Profil_i(g_i)}$ puis, on choisit ensuite $\mathbf{p_{f\text{-}e}}$ tel que $\mathbf{Profil_{f\text{-}e}(g) \neq Profil_{f\text{-}e}(g_m)}$.

(3) Cas où f-e-1 < m

Dans le cas où f-e-1 < m, on choisit $\mathbf{p_{f\text{-}e}}$ tel que les deux conditions suivantes soient satisfaites :

(3.1) Première condition.

On calcule $\mathbf{Profil_{f\text{-}e\text{-}1}(g_{f\text{-}e\text{-}1})}$ par rapport aux f-e-1 premiers facteurs premiers, de $\mathbf{p_1}$ à $\mathbf{p_{f\text{-}e\text{-}1}}$, Deux cas sont alors à considérer. Selon l'un ou l'autre de ces deux cas, la première condition sera différente.

Si $\mathbf{Profil_{f\text{-}e\text{-}1}(g_{f\text{-}e\text{-}1})}$ est plat, on choisit $\mathbf{p_{f\text{-}e}}$ tel qu'il satisfasse à la première condition d'être complémentaire de $\mathbf{p_1}$ par rapport à $\mathbf{g_{f\text{-}e\text{-}1}}$ (première condition selon le premier cas) sinon, on choisit parmi les **f-e-1** nombres de bases de $\mathbf{g_1}$ à $\mathbf{g_{m-1}}$ et toutes leurs combinaisons multiplicatives le nombre, ci-après dénommé **g,** tel que $\mathbf{Profil_i(g) = Profil_{f\text{-}e\text{-}1}(g_{f\text{-}e\text{-}1})}$ puis, on choisit ensuite $\mathbf{p_{f\text{-}e}}$ tel qu'il satisfasse à la condition d'être tel que $\mathbf{Profil_{f\text{-}e}(g) \neq Profil_{f\text{-}e}(g_m)}$, (première condition selon le deuxième cas)

(3.2) Deuxième condition

On sélectionne parmi l'ensemble des derniers nombres de bases de $\mathbf{g_{f\text{-}e}}$ à $\mathbf{g_m}$ ceux dont le profil $\mathbf{Profil_{f\text{-}e\text{-}1}(g_i)}$ est plat puis, on choisit $\mathbf{p_{f\text{-}e}}$ tel qu'il satisfasse à la condition d'être complémentaire de $\mathbf{p_1}$ par rapport à chacun des nombres de bases ainsi sélectionnés (deuxième condition).

Choix des e facteurs premiers congrus à 1 modulo 4

Pour produire les **e** facteurs premiers congrus à 1 modulo 4, on évalue chaque candidat facteur premier **p** , de $\mathbf{p_{f\text{-}e}}$ à $\mathbf{p_f}$, en lui faisant subir les deux

tests successifs suivants.

(1) Premier test

On calcule le symbole de Legendre de chaque nombre de base $\mathbf{g_i}$, de $\mathbf{g_1}$ à $\mathbf{g_m}$, par rapport au facteur premier **p** candidat,

- si le symbole de Legendre est égal à -1, on rejette le candidat **p**,
- si le symbole de Legendre est égal à +1, on poursuit l'évaluation du candidat **p** en passant au nombre de base suivant puis, lorsque le dernier nombre de base a été pris en compte on passe au deuxième test,

(2) Deuxième test,

On calcule un nombre entier **t** tel que p-1 est divisible par 2^t mais pas par 2^{t+1} puis, on calcule un entier **s** tel que $\mathbf{s = (p-1+2^t)/2^{t+1}}$.

On applique la clé $\langle \mathbf{s, p} \rangle$ à chaque valeur publique $\mathbf{G_i}$ pour obtenir un résultat **r**

$$\mathbf{r \equiv G_i^{\,s} \bmod p}$$

Si **r** est égal à $\mathbf{g_i}$ ou $-\mathbf{g_i}$, on poursuit le deuxième test en passant à la valeur publique $\mathbf{G_{i+1}}$ suivante.

Si **r** est différent de $\mathbf{g_i}$ ou $-\mathbf{g_i}$, on calcule un facteur **u** en appliquant l'algorithme ci-après spécifié pour un indice **ii** allant de 1 à t-2. L'algorithme met en oeuvre deux variables : **w** initialisée par **r** et $\mathbf{jj = 2^{ii}}$ prenant des valeurs allant de 2 à 2^{t-2}, ainsi qu'un nombre **b** obtenu par l'application de la clé $\langle \mathbf{(p-1)/2^t, p} \rangle$ à un résidu non quadratique de CG(p). L'algorithme consiste à répéter autant que nécessaire, la séquence suivante:

- Etape 1 : on calcule $w^2/G_i \pmod p$.
- Etape 2 : on élève le résultat à la puissance 2^{t-ii-1}. Deux cas sont à considérer.

Premier cas

Si on obtient +1, on passe à la valeur publique $\mathbf{G_{i+1}}$ suivante et on poursuit le deuxième test pour cette valeur publique.

Deuxième cas.

Si on obtient -1, on calcule jj = 2^{ii} puis, on remplace w par $w.b^{jj}$ (mod p). Ensuite, on poursuit l'algorithme pour la valeur suivante de l'indice ii.

A l'issue de l'algorithme, la valeur figurant dans la variable jj permet de calculer un nombre entier u par la relation jj = 2^{t-u} puis, on calcule l'expression t-u. Deux cas se présentent :

- si t-u < k , on rejette le candidat **p**
- si t-u ≥ k, on continue l'évaluation du candidat **p** en passant à la valeur publique $\mathbf{G_{i+1}}$ suivante puis, en poursuivant le deuxième test.

Le candidat **p** est accepté comme facteur premier congru à 1 modulo 4 si à l'issue du deuxième test, pour toutes les **m** valeurs publiques $\mathbf{G_i}$, il n'a pas été rejeté.

Application aux valeurs publiques et privées de GQ2

La présente invention concerne également un procédé (procédé GQ2) faisant application du procédé qui vient d'être décrit et qui permet, rappelons le, de produire **f** facteurs premiers $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$ ayant des propriétés particulières. Le procédé faisant application du procédé qui vient d'être décrit est destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité,

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $\mathbf{Q_1}$, $\mathbf{Q_2}$, ... $\mathbf{Q_m}$ et publiques $\mathbf{G_1}$, $\mathbf{G_2}$, ... $\mathbf{G_m}$ (**m** étant supérieur ou égal à 1),
- le module public **n** constitué par le produit desdits **f** facteurs premiers $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$ (**f** étant supérieur ou égal à 2),
- l'exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n .$$

Ledit exposant **v** est tel que

$$v = 2^k$$

où **k** est un paramètre de sécurité plus grand que 1 .

Ladite valeur publique G_i est le carré g_i^2 du nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$. Le nombre de base g_i est tel que les deux équations :

$$x^2 \equiv g_i \mathbf{mod}\ n \quad \text{et} \quad x^2 \equiv -g_i \mathbf{mod}\ n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n** et tel que l'équation :

$$x^v \equiv g_i^2 \mathbf{mod}\ n$$

a des solutions en x dans l'anneau des entiers modulo **n.**

Ledit procédé met en œuvre selon les étapes suivantes une entité appelée témoin. Ladite entité témoin dispose des **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs privées Q_i et de l'exposant public **v** .

Le témoin calcule des engagements **R** dans l'anneau des entiers modulo **n** . Chaque engagement est calculé :

- soit en effectuant des opérations du type

$$R \equiv r^v \mathbf{mod}\ n$$

où **r** est un aléa tel que $0 < r < n$,

- soit en effectuant des opérations du type

$$R_i \equiv r_i^v \mathbf{mod}\ p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \ldots r_f\}$, puis en appliquant la méthode des restes chinois.

Le témoin reçoit un ou plusieurs défis **d**. Chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires. Le témoin calcule à partir de

chaque défi **d** une réponse **D**,

- soit en effectuant des opérations du type :

$$\mathbf{D \equiv r \cdot Q_1^{\,d1} \cdot Q_2^{\,d2} \cdot \ldots Q_m^{\,dm} \bmod n}$$

- soit en effectuant des opérations du type :

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

puis, en appliquant la méthode des restes chinois.

Le procédé est tel qu'il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

De préférence, pour mettre en oeuvre, comme il vient d'être décrit, les couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$, on utilise les facteurs premiers $p_1, p_2, \ldots p_f$ et/ou les paramètres des restes chinois, les nombres de bases $g_1, g_2, \ldots g_m$ et/ou les valeurs publiques $G_1, G_2, \ldots G_m$ pour calculer :

- soit les valeurs privées $Q_1, Q_2, \ldots Q_m$ en extrayant une **k ième** racine carrée modulo **n** de G_i , ou en prenant l'inverse d'une **k ième** racine carrée modulo **n** de G_i,

- soit les **f.m** composantes privées $Q_{i,j}$ des valeurs privées $Q_1, Q_2, \ldots Q_m$, telles que $Q_{i,j} \equiv Q_i \pmod{p_j}$,

Plus particulièrement, pour calculer les **f.m** composantes privées $Q_{i,j}$ des valeurs privées $Q_1, Q_2, \ldots Q_m$:

- on applique la clé $\langle s, p_j \rangle$ pour calculer **z** tel que

$$\mathbf{z \equiv G_i^{\,s} \pmod{p_j}}$$

- et on utilise les valeurs **t** et **u** .

Les valeurs **t** et **u** sont calculées comme il a été indiqué ci-dessus dans le cas où p_j est congru à 1 modulo 4. Les valeurs **t** et **u** sont prises respectivement égales à 1 (t=1) et 0 (u=0) dans le cas où p_j est congru à 3 modulo 4.

Si la valeur **u** est nul, on considère l'ensemble des nombres zz tels que :

• • • zz soit égale à z ou tel que

• • • zz soit égale au produit (mod p_j) de z par chacune des 2^{ii-t} racines 2^{ii}ièmes primitives de l'unité, ii allant de 1 à min(k,t) .

Si **u** est positif, on considère l'ensemble des nombres zz tels que zz soit égale au produit (mod p_j) de za par chacune des 2^k racines 2^kièmes de l'unité, za désignant la valeur de la variable w à l'issue de l'algorithme ci-dessus décrit.

On en déduit au moins une valeur de la composante $\mathbf{Q_{i,j}}$. Elle est égale à zz lorsque l'équation $\mathbf{G_i \equiv Q_i^v \bmod n}$ est utilisée ou bien elle est égale à l'inverse de zz modulo p_j de zz lorsque l'équation $\mathbf{G_i \cdot Q_i^v \equiv 1 \cdot \bmod n}$ est utilisée.

Description

Rappelons l'objectif de la technologie GQ : l'authentification dynamique d'entités et de messages associés, ainsi que la signature numérique de messages.

La version classique de la technologie GQ fait appel à la technologie RSA. Mais, si la technologie RSA dépend bel et bien de la factorisation, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites « multiplicatives » contre diverses normes de signature numérique mettant en œuvre la technologie RSA.

Dans le cadre de la technologie GQ2, la présente partie de l'invention porte plus précisément sur la production des jeux de clés GQ2 destinés à assurer l'authentification dynamique et la signature numérique. La technologie GQ2 ne fait pas appel à la technologie RSA. L'objectif est double : d'une part, améliorer les performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La clé privée GQ2 est la factorisation du module n. Toute attaque au niveau des triplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 concurrence la technologie RSA.

La technologie GQ2 utilise un ou plusieurs petits nombres entiers plus grands que 1, disons m petits nombres entiers ($m \geq 1$) appelés « nombres de base » et notés par g_i. Puis, on choisit une clé publique de vérification $\langle v, n \rangle$ de la manière suivante. L'exposant public de vérification v est 2^k où k est un petit nombre entier plus grand que 1 ($k \geq 2$). Le module public n est le produit d'au moins deux facteurs premiers plus grands que les nombres de base, disons f facteurs premiers ($f \geq 2$) notés par p_j, de $p_1 \ldots p_f$. Les f facteurs premiers sont choisis de façon à ce que le module public n ait les propriétés

suivantes par rapport à chacun des m nombres de base de g_1 à g_m.

- D'une part, les équations (1) et (2) n'ont pas de solution en x dans l'anneau des entiers modulo n, c'est-à-dire que g_i et $-g_i$ sont deux résidus non quadratiques (mod n).

$$x^2 \equiv g_i \pmod{n} \qquad (1)$$

$$x^2 \equiv -g_i \pmod{n} \qquad (2)$$

- D'autre part, l'équation (3) a des solutions en x dans l'anneau des entiers modulo n.

$$x^{2^k} \equiv g_i^2 \pmod{n} \qquad (3)$$

Par la suite, ces propriétés sont encore appelées les principes GQ2.

La clé publique de vérification $\langle v, n \rangle$ étant fixée selon les nombres de base de g_1 à g_m avec $m \geq 1$, chaque nombre de base g_i détermine un couple de valeurs GQ2 comprenant une valeur publique G_i et une valeur privée Q_i: soit m couples notés de G_1 Q_1 à G_m Q_m. La valeur publique G_i est le carré du nombre de base g_i: soit $G_i = g_i^2$. La valeur privée Q_i est une des solutions à l'équation (3) ou bien l'inverse (mod n) d'une telle solution.

De même que le module n se décompose en f facteurs premiers, l'anneau des entiers modulo n se décompose en f corps de Galois, de CG(p_1) à CG(p_f). Voici les projections des équations (1), (2) et (3) dans CG(p_j).

$$x^2 \equiv g_i \pmod{p_j} \qquad (1.a)$$

$$x^2 \equiv -g_i \pmod{p_j} \qquad (2.a)$$

$$x^{2^k} \equiv g_i^2 \pmod{p_j} \qquad (3.a)$$

Chaque valeur privée Q_i peut se représenter de manière unique par f composantes privées, une par facteur premier : $Q_{i,j} \equiv Q_i \pmod{p_j}$. Chaque composante privée $Q_{i,j}$ est une solution à l'équation (3.a) ou bien l'inverse (mod p_j) d'une telle solution. Après que toutes les solutions possibles à chaque équation (3.a) aient été calculées, la technique des restes chinois permet d'établir toutes les valeurs possibles pour chaque valeur privée Q_i à partir de f composantes de $Q_{i,1}$ à $Q_{i,f}$: Q_i = Restes Chinois ($Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$) de manière à obtenir toutes les solutions possibles à l'équation (3).

Voici la technique des restes chinois : soient deux nombres entiers positifs premiers entre eux a et b tels que $0 < a < b$, et deux composantes X_a de 0 à a–1 et X_b de 0 à b–1 ; il s'agit de déterminer X = Restes Chinois (X_a, X_b), c'est-à-dire, le nombre unique X de 0 à $a.b$–1 tel que $X_a \equiv X \pmod{a}$ et $X_b \equiv X \pmod{b}$. Voici le paramètre des restes chinois : $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$. Voici l'opération des restes chinois : $\varepsilon \equiv X_b \pmod{a}$; $\delta = X_a - \varepsilon$; si δ est négatif, remplacer δ par $\delta + a$; $\gamma \equiv \alpha . \delta \pmod{a}$; $X = \gamma . b + X_b$.

Lorsque les facteurs premiers sont rangés dans l'ordre croissant, du plus petit p_1 au plus grand p_f, les paramètres des restes chinois peuvent être les suivants (il y en a f–1, c'est-à-dire, un de moins que de facteurs premiers). Le premier paramètre des restes chinois est $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$. Le second paramètre des restes chinois est $\beta \equiv \{p_1.p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$. Le i ième paramètre des restes chinois est $\lambda \equiv \{p_1.p_2. \ldots p_{i-1} \pmod{p_i}\}^{-1} \pmod{p_i}$. Et ainsi de suite. Ensuite, en f–1 opérations des restes chinois, on établit un premier résultat (mod p_2 fois p_1) avec le premier paramètre, puis, un second résultat (mod $p_1.p_2$ fois p_3) avec le second paramètre, et ainsi de suite, jusqu'à un résultat (mod $p_1. \ldots p_{f-1}$ fois p_f), c'est-à-dire, (mod n).

L'objet de l'invention est une méthode pour produire au hasard n'importe quel jeu de clés GQ2 parmi tous les jeux possibles, à savoir :

- produire au hasard n'importe quel module parmi tous les modules GQ2 possibles, c'est-à-dire, les modules assurant que, pour chacun des m nombres de base g_i, les équations (1) et (2) n'ont pas de solution en x dans l'anneau des entiers modulo n alors que l'équation (3) en a.
- calculer toutes les solutions possibles à chacune des équations (3.a). La technique des restes chinois permet ensuite d'obtenir une valeur privée Q_i à partir de chaque jeu de f composantes de $Q_{i,1}$ à $Q_{i,f}$ de manière à obtenir n'importe quelle solution en x à l'équation (3) parmi toutes les solutions possibles.

$$Q_i = \text{Restes Chinois } (Q_{i,1}, Q_{i,2}, \ldots Q_{i,f})$$

Pour appréhender le problème, puis, comprendre la solution que nous

donnons au problème, c'est-à-dire, l'invention, nous analysons tout d'abord l'applicabilité des principes de la technologie GQ2. Commençons par rappeler la notion de rang dans un corps de Galois CG(p) afin d'étudier les fonctions « élever au carré dans CG(p) » et « prendre une racine carrée d'un résidu quadratique dans CG(p) ». Puis, analysons l'existence et le nombre de solutions en x dans CG(p) aux équations (1.a), (2.a) et (3.a).

Rang des éléments dans CG(p)

Soit un nombre premier impair p et un nombre entier positif a plus petit que p. Définissons la suite $\{X\}$.

$$\{X\} \equiv \{x_i = a ; \text{puispouri} \geq 1,\ x_{i+1} \equiv a x_i \pmod{p}\}$$

Calculons le terme pour l'indice $i+p$ et utilisons le théorème de Fermat.

$$x_{i+p} \equiv a^p x_i \equiv a x_i \equiv x_{i+1} \pmod{p}$$

Par conséquent, la période de la suite $\{X\}$ est $p-1$ ou un diviseur de $p-1$. Cette période dépend de la valeur de a. Par définition, cette période est appelée « le rang de a (mod p) ». C'est l'indice d'apparition de l'unité dans la suite $\{X\}$.

$$x_{\text{rang}(a,p)} \equiv 1 \pmod{p}$$

Par exemple, lorsque $(p-1)/2$ est un nombre premier impair p', le corps de Galois CG(p) comporte un seul élément de rang 1 : c'est 1, un seul élément de rang 2 : c'est -1, $p'-1$ éléments de rang p', $p'-1$ éléments de rang $2.p'$, c'est-à-dire, de rang $p-1$.

Les éléments de CG(p) ayant pour rang $p-1$ sont appelés les éléments « primitifs » ou encore, « générateurs » de CG(p). La dénomination est due au fait que leurs puissances successives dans CG(p), c'est-à-dire, les termes de la suite $\{X\}$ pour les indices allant de 1 à $p-1$, forment une permutation de tous les éléments non nuls de CG(p).

Soit un élément primitif y de CG(p). Evaluons le rang de l'élément y^i (mod p) en fonction de i et de $p-1$. Lorsque i est premier avec $p-1$, c'est $p-1$. Lorsque i divise $p-1$, c'est $(p-1)/i$. Dans tous les cas, c'est $(p-1)/\text{pgcd}(p-1, i)$.

La fonction d'Euler est notée par φ. Par définition, n étant un nombre entier positif, $\varphi(n)$ est le nombre de nombres entiers positifs, plus petits que n et premiers avec n. Dans le corps CG(p), il y a donc $\varphi(p-1)$ éléments primitifs.

A titre d'illustration, voici la base de la technologie RSA. Le module public n est le produit de f facteurs premiers, de p_1 à p_f avec $f \geq 2$, tel que pour chaque facteur premier p_j, l'exposant public v est premier avec p_j-1. La clé $\langle v, p_j \rangle$ respecte le rang des éléments de CG(p_j) : elle les permute. La permutation inverse s'obtient par une clé $\langle s_j, p_j \rangle$ telle que p_j-1 divise $v.s_j-1$.

Carrés et racines carrées dans CG(p)

Les éléments x et $p-x$ ont le même carré dans CG(p). La clé $\langle 2, p \rangle$ ne permute pas les éléments de CG(p) parce que $p-1$ est pair. Pour chaque nombre premier p, définissons un nombre entier t de la manière suivante : $p-1$ est divisible par 2^t, mais pas par 2^{t+1}, c'est-à-dire que p est congru à 2^t+1 (mod 2^{t+1}). Par exemple, $t = 1$ lorsque p est congru à 3 (mod 4) ; $t = 2$ lorsque p est congru à 5 (mod 8) ; $t = 3$ lorsque p est congru à 9 (mod 16) ; $t = 4$ lorsque p est congru à 17 (mod 32) ; et ainsi de suite. Chaque nombre premier impair figure dans une et une seule catégorie : p figure dans la t ième catégorie. En pratique, si l'on considère un assez grand nombre de nombres premiers successifs, environ un sur deux figure dans la première catégorie, un sur quatre dans la deuxième, un sur huit dans la troisième, un sur seize dans la quatrième, et ainsi de suite ; en résumé, un sur 2^t en moyenne figure dans la t ième catégorie.

Considérons le comportement de la fonction « élever au carré dans CG(p) » selon la parité du rang de l'argument.

- Il y a un seul élément fixe : c'est 1. Le carré de tout autre élément de rang impair est un autre élément ayant le même rang. Par conséquent, la clé $\langle 2, p \rangle$ permute l'ensemble des $(p-1)/2^t$ éléments de rang impair. Le nombre de cycles de permutation dépend de la factorisation de $(p-1)/2^t$. Par exemple, lorsque $(p-1)/2^t$ est un nombre premier p', il y a

un grand cycle de permutation comportant $p'-1$ éléments.

- Le carré de tout élément de rang pair est un autre élément dont le rang est divisé par deux. Par conséquent, les éléments de rang pair se répartissent sur $(p-1)/2^t$ branches ; chaque élément non nul de rang impair porte une branche de longueur t comportant 2^t-1 éléments, à savoir : un élément de rang divisible par deux mais pas par quatre, puis, si $t \geq 2$, deux éléments de rang divisible par quatre mais pas par huit, puis, si $t \geq 3$, quatre éléments de rang divisible par huit mais pas par seize, puis, si $t \geq 4$, huit éléments de rang divisible par seize mais pas par 32, et ainsi de suite. Les 2^{t-1} extrémités de chaque branche sont des résidus non quadratiques ; leur rang est divisible par 2^t.

Les figures 1A à 1D illustrent la fonction « élever au carré dans CG(p) » par un graphe orienté où chacun des $p-1$ éléments non nuls du corps trouve sa place : les résidus non quadratiques sont en blanc et les résidus quadratiques en noir ; parmi les résidus quadratiques, les éléments de rang impair sont encerclés.

Ces figures présentent respectivement :

- figure 1A : cas où p est congru à 3 (mod 4) ;
- figure 1B : cas où p est congru à 5 (mod 8) ;
- figure 1 C : cas où p est congru à 9 (mod 16) ;
- figure 1D : cas où p est congru à 17 (mod 32).

Voyons comment calculer une solution en x à l'équation $x^2 \equiv a \pmod{p}$ sachant que a est un résidu quadratique de CG(p), c'est-à-dire, comment « prendre une racine carrée dans CG(p) ». Il y a bien sûr plusieurs façons d'obtenir le même résultat : le lecteur pourra avantageusement consulter les pages 31 à 36 du livre de Henri Cohen, *a Course in Computational Algebraic Number Theory*, publié en 1993 par Springer à Berlin comme le volume 138 de la série *Graduate Texts in Mathematics* (GTM 138).

Calculons un nombre entier $s = (p-1+2^t)/2^{t+1}$ pour établir une clé $\langle s, p \rangle$.

Soit : $\langle (p+1)/4, p\rangle$ lorsque p est congru à 3 (mod 4), $\langle (p+3)/8, p\rangle$ lorsque p est congru à 5 (mod 8), $\langle (p+7)/16, p\rangle$ lorsque p est congru à 9 (mod 16), $\langle (p+15)/32, p\rangle$ lorsque p est congru à 17 (mod 32), et ainsi de suite.

- La clé $\langle s, p\rangle$ donne la racine carrée de rang impair de n'importe quel élément de rang impair. En effet, dans CG(p), r^2/a vaut a élevé à la puissance $(2.(p-1+2^t)/2^{t+1})-1 = (p-1)/2^t$. Par conséquent, lorsque a est sur un cycle, la clé $\langle s, p\rangle$ transforme a en une solution que nous nommons w. L'autre solution est $p-w$.
- D'une manière générale, la clé $\langle s, p\rangle$ transforme tout résidu quadratique a en une première approximation de solution que nous nommons r. Voici deux points clés, puis, l'ébauche d'une méthode pour améliorer pas à pas l'approximation jusqu'à une racine carrée de a.
  - D'une part, puisque a est un résidu quadratique, la clé $\langle 2^{t-1}, p\rangle$ transforme certainement r^2/a en 1.
  - D'autre part, supposons que nous connaissons un résidu non quadratique de CG(p) que nous nommons y ; la clé $\langle (p-1)/2^t, p\rangle$ transforme y en un élément que nous nommons b : c'est une racine 2^{t-1} ième de -1 ; en effet, $y^{(p-1)/2} \equiv -1 \pmod{p}$. Par conséquent, dans CG(p), le groupe multiplicatif des 2^t racines 2^t ièmes de l'unité est isomorphe au groupe multiplicatif des puissances de b pour les exposants de 1 à 2^t.
  - Pour se rapprocher d'une racine carrée de a, élevons r^2/a à la puissance 2^{t-2} (mod p) : le résultat est +1 ou −1. La nouvelle approximation reste r si le résultat est +1 ou bien devient $b.r$ (mod p) si le résultat est −1. Par conséquent, la clé $\langle 2^{t-2}, p\rangle$ transforme certainement la nouvelle approximation en 1. On peut continuer à se rapprocher : au prochain pas, on ajustera s'il le faut en multipliant par b^2 (mod p) ; et ainsi de suite.

L'algorithme suivant établit des approximations successives pour aboutir à une racine carrée de a à partir des nombres entiers r et b définis ci-dessus ;

il utilise deux variables entières : w initialisée par r pour représenter les approximations successives et jj prenant des valeurs parmi les puissances de 2, de 2 à 2^{t-2}.

Pour i allant de 1 à $t-2$, répéter la séquence suivante :

- Calculer $w^2/a \pmod p$, puis, élever le résultat à la puissance $2^{t-i-1} \pmod p$: on doit obtenir +1 ou −1. Lorsque l'on obtient −1, calculer $jj = 2^i$, puis, remplacer w par $w.b^{jj} \pmod p$. Lorsque l'on obtient +1, ne rien faire.

A l'issue du calcul, w et $p-w$ sont les deux racines carrées de a dans CG(p). En outre, nous apprenons que le rang de a dans CG(p) est divisible par $2^t/jj$ mais pas par $2^{t+1}/jj$. La pertinence de cette remarque apparaîtra par la suite.

Analyse des principes de la technologie GQ2 dans CG(p)

Soit deux nombres entiers g et k plus grands que 1 et un nombre premier p plus grand que g. Analysons l'existence et le nombre de solutions en x dans CG(p) aux équations (1.a), (2.a) et (3.a).

Dans le corps de Galois CG(p), distinguons différents cas selon la valeur de t, c'est-à-dire, selon la puissance de deux qui divise $p-1$. Rappelons que $p-1$ est divisible par 2^t, mais pas par 2^{t+1}, c'est-à-dire que p est congru à $2^t+1 \pmod{2^{t+1}}$. L'analyse précédente nous donne une idée assez précise du problème posé ainsi qu'une ébauche de solution.

Lorsque $t = 1$, p est congru à 3 (mod 4). Les symboles de Legendre de g et $-g$ par rapport à p sont différents ; tout résidu quadratique de CG(p) a deux racines carrées dans CG(p) : l'une est un résidu quadratique et l'autre un résidu non quadratique. D'une part, une des deux équations (1.a) ou (2.a) a deux solutions en x dans CG(p) et l'autre n'en à pas. D'autre part, l'équation (3.a) a deux solutions en x dans CG(p) quelle que soit la valeur de k.

Lorsque $t = 2$, p est congru à 5 (mod 8). Deux cas se présentent selon le symbole de Legendre de g par rapport à p. Lorsque le symbole vaut −1, g et $-g$ sont deux résidus non quadratiques de CG(p) : les trois équations (1.a), (2.a) et (3.a) n'ont pas de solution en x dans CG(p). Lorsque le

symbole vaut +1, g et $-g$ sont deux résidus quadratiques de CG(p), chaque équation (1.a) et (2.a) a deux solutions en x dans CG(p) ; de plus, le rang de g^2 dans CG(p) est impair, ce qui implique que quelle que soit la valeur de k, l'équation (3.a) a quatre solutions en x dans CG(p) dont une seule de rang impair.

La figure 2 illustre les solutions à l'équation (3.a) avec $k = 6$ et p congru à 5 (mod 8), soit $t = 2$. Remarquons que, parce que le symbole de Legendre de 2 par rapport à p congru à 5 (mod 8) vaut -1, $2^{(p-1)/4}$ (mod p) est alors une racine carrée de -1. On a donc :

$p \equiv 5 \pmod 8$; par conséquent : $(2|p) = -1$

$p \equiv 2^{\frac{p-1}{4}} \pmod p$; donc $b^2 \equiv -1 \pmod p$

Lorsque $t = 3$, p est congru à 9 (mod 16). Considérons le symbole de Legendre de g par rapport à p. Lorsque le symbole vaut -1, g et $-g$ sont deux résidus non quadratiques de CG(p) : les trois équations (1.a), (2.a) et (3.a) n'ont pas de solution en x dans CG(p). Lorsque le symbole vaut +1, g et $-g$ sont deux résidus quadratiques de CG(p) ; chaque équation (1.a) et (2.a) a deux solutions en x dans CG(p) ; l'existence de solutions en x à l'équation (3.a) dépend du rang de g^2 dans CG(p) : ce rang est impair ou divisible par deux, mais pas par quatre. Lorsque le rang de g^2 dans CG(p) est divisible par deux, mais pas par quatre, l'équation (3.a) a quatre solutions en x dans CG(p) pour $k = 2$; elle n'en a pas pour $k \geq 3$. Lorsque le rang de g^2 dans CG(p) est impair, l'équation (3.a) a quatre solutions en x dans CG(p) pour $k = 2$ et huit pour $k \geq 3$; dans les deux cas, une seule est de rang impair.

Lorsque $t = 4$, p est congru à 17 (mod 32). Considérons le symbole de Legendre de g par rapport à p. Lorsque le symbole vaut -1, g et $-g$ sont deux résidus non quadratiques de CG(p) : les trois équations (1.a), (2.a) et (3.a) n'ont pas de solution en x dans CG(p). Lorsque le symbole vaut +1, g et $-g$ sont deux résidus quadratiques de CG(p) ; chaque équation (1.a) et (2.a) a deux solutions en x dans CG(p) ; l'existence de solutions en x à

l'équation (3.a) dépend du rang de g^2 dans CG(p) : ce rang est impair ou divisible par deux ou quatre, mais pas par huit. Lorsque le rang de g^2 dans CG(p) est divisible par quatre, mais pas par huit, l'équation (3.a) a quatre solutions en x dans CG(p) pour $k = 2$; elle n'en a pas pour $k \geq 3$. Lorsque le rang de g^2 dans CG(p) est divisible par deux, mais pas par quatre, l'équation (3.a) a quatre solutions en x dans CG(p) pour $k = 2$ ou huit pour $k = 3$; elle n'en a pas pour $k \geq 4$. Lorsque le rang de g^2 dans CG(p) est impair, l'équation (3.a) a quatre solutions en x dans CG(p) pour $k = 2$, huit pour $k = 3$ et seize pour $k \geq 4$; dans les trois cas, une seule est de rang impair.

Et ainsi de suite, de sorte que le cas où p est congru à 1 (mod 4) peut se résumer comme suit.

Lorsque p est congru à 1 (mod 4), considérons le symbole de Legendre de g par rapport à p. Lorsque le symbole vaut -1, g et $-g$ sont deux résidus non quadratiques de CG(p) : les trois équations (1.a), (2.a) et (3.a) n'ont pas de solution en x dans CG(p). Lorsque le symbole vaut $+1$, g et $-g$ sont deux résidus quadratiques de CG(p) ; chaque équation (1.a) et (2.a) a deux solutions en x dans CG(p). Définissons le nombre entier u : le rang de g^2 dans CG(p) est divisible par 2^u, mais pas par 2^{u+1} ; la valeur de u figure parmi les $t-1$ valeurs possibles, de 0 à $t-2$. L'existence et le nombre de solutions en x dans CG(p) à l'équation (3.a) dépend des valeurs de k, t et u. Lorsque u est positif et k est supérieur à $t-u$, l'équation (3.a) n'a pas de solution en x dans CG(p). Lorsque u est nul et k supérieur à t, l'équation (3.a) a 2^t solutions en x dans CG(p). Lorsque k inférieur ou égal à $t-u$, l'équation (3.a) a 2^k solutions en x dans CG(p).

Applicabilité des principes GQ2 dans les anneaux d'entiers modulo

Pour que l'équation (1), respectivement (2), n'ait pas de solution en x dans l'anneau des entiers modulo n, il faut et il suffit que, pour au moins un des facteurs premiers p, de p_1 à p_f, l'équation (1.a), respectivement (2.a), n'ait pas de solution en x dans CG(p).

Pour que l'équation (3) ait des solutions en x dans l'anneau des entiers modulo n, il faut et il suffit que, pour chacun des facteurs premiers p, de p_1 à p_f, l'équation (3.a) ait des solutions en x dans CG(p).

L'équation (3) interdit tout facteur premier p congru à 1 (mod 4) dès que pour l'un des nombres de base g, de g_1 à g_m : ou bien, le symbole de Legendre de g par rapport à p est égal à -1 ; ou bien, le symbole de Legendre de g par rapport à p est égal à $+1$ avec la condition : u positif et supérieur à $t-k$. Pour qu'un facteur premier p congru à 1 (mod 4) soit possible, il doit remplir l'une des deux conditions suivantes pour chacun des nombres de base g, de g_1 à g_m, selon les deux nombres entiers t et u définis ci-dessus. Ou bien, le rang de $G = g^2$ est impair dans CG(p), c'est-à-dire, $u = 0$, quelle que soit la valeur de k. Ou bien, le rang de $G = g^2$ est pair dans CG(p), c'est-à-dire, $u > 0$, et il satisfait la condition : $u + k \leq t$.

Un produit de facteurs premiers congrus à 1 (mod 4) ne peut assurer l'ensemble des principes de la technologie GQ2. Chaque module GQ2 doit avoir au moins deux facteurs premiers congrus à 3 (mod 4) tels que, pour chaque nombre de base g, le symbole de Legendre de g par rapport à l'un diffère du symbole de Legendre de g par rapport à l'autre. Lorsque tous les facteurs premiers sont congrus à 3 (mod 4), on dira que le **module GQ2** est **basique**. Lorsqu'en plus d'au moins deux facteurs premiers congrus à 3 (mod 4), le module inclut un ou plusieurs facteurs premiers congrus à 1 (mod 4), on dira que le **module GQ2** est **mixte**.

Construction systématique de modules GQ2

Au départ, il faut fixer les contraintes globales à imposer au module n : une taille en bits (par exemple, 512 ou 1024 bits) ainsi qu'un nombre de bits successifs à 1 en poids forts (au moins un bien sûr, typiquement 16 ou 32 bits), un nombre f de facteurs premiers et un nombre e (pouvant être nul) de facteurs premiers devant être congrus à 1 (mod 4) ; les autres facteurs premiers, soit $f-e$ facteurs, au moins deux, doivent être congrus à 3 (mod 4). Le module n sera le produit de f facteurs premiers de tailles voisines.

Lorsque $e = 0$, on obtient un module GQ2 basique ; lorsque $e > 0$, on obtient un module GQ2 mixte. Un module basique est le produit de facteurs premiers tous congrus à 3 (mod 4). Un module GQ2 mixte apparaît donc comme le produit d'un module GQ2 basique par un ou plusieurs autres facteurs premiers congrus à 1 (mod 4). On produit d'abord des facteurs premiers congrus à 3 (mod 4). Ensuite, si $e > 0$, on produit des facteurs premiers congrus à 1 (mod 4).

Pour l'efficacité de la construction de modules GQ2, il vaut bien mieux sélectionner chaque candidat avant de chercher à savoir s'il est premier.

Notés par g_1 g_2 ... , les nombres de base figurent typiquement parmi les premiers nombres premiers : 2, 3, 5, 7, ... Faute d'indication contraire, les m nombres de base sont les m premiers nombres premiers : $g_1 = 2$, $g_2 = 3$, $g_3 = 5$, $g_4 = 7$, ... Toutefois, notons les remarques suivantes : il faut éviter 2 si l'on escompte un facteur congru à 5 (mod 8) ; il faut éviter 3 si l'on doit utiliser la clé publique $\langle 3, n \rangle$ comme clé publique de vérification RSA.

Choix de f–e facteurs premiers congrus à 3 (mod 4)

A partir du deuxième facteur, le programme demande et utilise un nombre de base par facteur. Pour le choix du dernier facteur congru à 3 (mod 4), le programme demande s'il y a d'autres nombres de base, c'est-à-dire, si m est égal ou supérieur à f–e, puis, si tel est le cas, demande et prend en compte les derniers nombres de base, de g_{f-e} à g_m. Pour formaliser le choix des facteurs premiers congrus à 3 (mod 4), nous avons introduit une notion de **profil** ; le profil caractérise un nombre entier g par rapport à un ensemble de facteurs premiers plus grands que g et congrus à 3 (mod 4).

- Lorsqu'un nombre entier g a le même symbole de Legendre par rapport à deux facteurs premiers, on dit que les facteurs premiers sont **équivalents** par rapport à g. Sinon, ils sont **complémentaires** par rapport à g.
- Noté par Profil$_f(g)$, le **profil** d'un nombre entier g par rapport à f facteurs premiers p_1 p_2 ... p_f est une séquence de f bits, un bit par facteur premier.

Le premier bit vaut 1 ; chaque bit suivant vaut 1 ou 0 selon que le facteur suivant est équivalent ou complémentaire de p_1 par rapport à g.

- Lorsque tous les bits d'un profil sont égaux à 1, on dit que le profil est **plat**. Dans un tel cas, tous les symboles de Legendre de g sont égaux à +1, ou bien, à –1. Lorsque le profil de g est non plat, les équations (1) et (2) n'ont pas de solution en x dans l'anneau des entiers modulo n.
- Par définition, le profil de g par rapport à un seul nombre premier congru à 3 (mod 4) est toujours plat. Cette extension permet de généraliser l'algorithme de choix des facteurs premiers congrus à 3 (mod 4).

Lorsque les profils de deux nombres de base g_1 et g_2 sont différents, ce qui implique au moins trois facteurs premiers congrus à 3 (mod 4), la connaissance des deux valeurs privées Q_1 et Q_2 induit la connaissance de deux décompositions différentes du module n. Lorsque les nombres de base sont des petits nombres premiers, le programme assure que les profils des $2^{f-e-1}-1$ combinaisons multiplicatives des $f-e-1$ premiers nombres de base sont tous différents : ils prennent toutes les valeurs possibles. La notion de profil ne s'étend pas aux facteurs premiers congrus à 1 (mod 4).

Premier facteur premier p_1 congru à 3 (mod 4) : Chaque candidat doit être congru à 3 (mod 4), sans autre contrainte particulière.

Deuxième facteur premier p_2 congru à 3 (mod 4) avec prise en compte du premier nombre de base g_1 : Chaque candidat doit être complémentaire de p_1 par rapport à g_1.

Troisième facteur premier p_3 congru à 3 (mod 4) avec prise en compte du deuxième nombre de base g_2 : Selon le profil de g_2 par rapport aux deux premiers facteurs premiers p_1 et p_2, deux cas se présentent. Lorsque $\text{Profil}_2(g_2)$ est plat, chaque candidat doit être complémentaire de p_1 par rapport à g_2. Sinon, on a $\text{Profil}_2(g_1) = \text{Profil}_2(g_2)$; chaque candidat doit alors assurer que $\text{Profil}_3(g_1) \neq \text{Profil}_3(g_2)$.

Choix du i ième facteur premier p_{i+1} congru à 3 (mod 4) avec prise en compte du nombre de base g_i: Selon le profil de g_i par rapport aux i

premiers facteurs premiers p_1, p_2, ... p_i, deux cas se présentent. Lorsque $\text{Profil}_i(g_i)$ est plat, chaque candidat doit être complémentaire de p_1 par rapport à g_i. Sinon, parmi les $i-1$ nombres de base g_1, g_2, ... g_{i-1} et toutes leurs combinaisons multiplicatives, $g_1.g_2$, ... , $g_1.g_2. \cdots g_{i-1}$, soit en tout $2^{i-1}-1$ nombres entiers, il existe un nombre entier g et un seul tel que $\text{Profil}_i(g_i) = \text{Profil}_i(g)$; chaque candidat doit alors assurer que $\text{Profil}_{i+1}(g_i) \neq \text{Profil}_{i+1}(g)$.

Dernier facteur premier p_{f-e} congru à 3 (mod 4) avec prise en compte du nombre de base g_{f-e-1} et des autres nombres de base de g_{f-e} à g_m : On prend en compte les contraintes dues au nombre de base g_{f-e-1}, tout comme ci-dessus. En outre, lorsque m est égal ou supérieur à $f-e$, chaque candidat doit assurer un profil non plat aux derniers nombres de base, de g_{f-e} à g_m, par rapport aux $f-e$ facteurs premiers. Chaque candidat doit être complémentaire de p_1 par rapport à tous les g_i pour lesquels $\text{Profil}_{f-e-1}(g_i)$ est plat.

En résumé, les facteurs premiers congrus à 3 (mod 4) sont choisis les uns en fonction des autres.

Pour i allant de 0 à $f-e-1$, pour choisir le $i+1$ ième facteur premier congru à 3 (mod 4), le candidat p_{i+1} doit passer avec succès l'examen suivant :

Si $i > m$ ou si $i = 0$, alors le candidat p_{i+1} n'a pas d'autre contrainte ; il est donc accepté.

Si $0 < i \leq m$, alors le candidat p_{i+1} doit prendre en compte le i ième nombre de base g_i. On calcule le profil $\text{Profil}_i(g_i)$ du nombre de base g_i par rapport aux i premiers facteurs premiers, de p_1 à p_i. Selon le résultat, un et un seul des deux cas suivants se présente :

- Si le profil est plat, alors le candidat p_{i+1} doit être complémentaire de p_1 par rapport à g_i ; sinon, il faut le rejeter.
- Sinon, parmi les $i-1$ nombres de base et toutes leurs combinaisons multiplicatives, il y a un et un seul nombre que nous nommons g tel que $\text{Profil}_i(g) = \text{Profil}_i(g_i)$; alors le candidat p_{i+1} doit être tel que $\text{Profil}_{i+1}(g) \neq \text{Profil}_{i+1}(g_i)$; sinon, il faut le rejeter.

Si $i+1 = f-e$ et $i < m$, c'est-à-dire, pour choisir le dernier facteur premier congru à 3 (mod 4) lorsqu'il reste des nombres de base, de g_{f-e} à g_m, qui n'ont pas encore été pris en compte, le candidat p_{f-e} doit les prendre en compte : parmi ces derniers nombres de base, on sélectionne ceux dont le profil $\text{Profil}_{f-e-1}(g_i)$ est plat ; le candidat p_{f-e} doit être complémentaire de p_1 par rapport à chacun des nombres de base ainsi sélectionnés ; sinon, il faut le rejeter.

Le candidat est accepté lorsqu'il a passé avec succès les tests appropriés.

Choix de *e* facteurs premiers congrus à 1 (mod 4)

Pour être acceptable, chaque candidat p congru à 1 (mod 4) doit remplir les conditions suivantes par rapport à chaque nombre de base de g_1 à g_m.

- Evaluons le symbole de Legendre de chaque nombre de base g_i par rapport à p. Si le symbole vaut -1, rejetons le candidat p pour passer à un autre candidat. Si le symbole vaut $+1$, poursuivons l'évaluation du candidat. Notons que si le nombre entier 2 est utilisé comme nombre de base, alors tous les candidats congrus à 5 (mod 8) doivent être écartés : le nombre de base 2 est incompatible avec un facteur congru à 5 (mod 8).
- Calculons un nombre entier $s = (p-1+2^t)/2^{t+1}$ pour établir une clé $\langle s, p \rangle$. Appliquons la clé $\langle s, p \rangle$ à chaque valeur publique G_i pour obtenir un résultat r. Deux cas se présentent.
  - Si r vaut g_i ou $-g_i$, alors $u = 0$. Dans ce cas et dans ce cas seulement, G_i est sur un cycle. Remarquons un cas trivial : G_i est sur un cycle dès lors que p est congru à 5 (mod 8) et que le symbole de Legendre de g_i par rapport à p vaut $+1$. Rappelons que $G_i = 4$ est impossible dans ce cas.
  - Si r ne vaut ni g_i ni $-g_i$, alors $u > 0$; notons que la clé $\langle (p-1)/2^t, p \rangle$ transforme tout résidu non quadratique y en un élément b qui est une racine 2^t ième primitive de l'unité. L'algorithme suivant calcule u à partir de r et b en utilisant deux variables entières : w initialisée

par r et jj prenant des valeurs de 2 à 2^{t-2}.

Pour i allant de 1 à $t-2$, répéter la séquence suivante :

- Calculer $w^2/G_i \pmod{p_j}$, puis, élever le résultat à la puissance $2^{t-i-1} \pmod{p_j}$: on doit obtenir +1 ou −1. Lorsque l'on obtient −1, calculer $jj = 2^i$, puis, remplacer w par $w.b^{jj} \pmod{p_j}$. Lorsque l'on obtient +1, ne rien faire.

A l'issue du calcul, la variable w a pour valeur g_i ou $-g_i$. De plus, nous savons que le rang de G_i dans $CG(p_j)$ est divisible par $2^t/jj$ mais pas par $2^{t+1}/jj$, c'est-à-dire que jj détermine la valeur de u par $jj = 2^{t-u}$. Lorsque v est plus grand que jj, c'est-à-dire, $k > t-u$, rejeter le candidat pour passer à un autre. Lorsque v est plus petit ou égal à jj, c'est-à-dire, $k \leq t-u$, poursuivre l'évaluation du candidat.

Lorsque les f facteurs premiers ont été produits, le module public n est le produit des f facteurs premiers $p_1, p_2, \ldots p_f$. L'entier non signé n peut se représenter par une séquence binaire ; cette séquence respecte les contraintes imposées au début du programme pour la taille en bits et pour le nombre de bits successifs à 1 en poids forts. Le choix des facteurs premiers assure les propriétés suivantes du module n par rapport à chacun des m nombres de base $g_1, g_2, \ldots g_m$. D'une part, les équations (1) et (2) n'ont pas de solution en x dans l'anneau des entiers modulo n. D'autre part, l'équation (3) a des solutions en x dans l'anneau des entiers modulo n.

En résumé, les facteurs premiers congrus à 1 (mod 4) sont choisis indépendamment les uns des autres. Alors que les facteurs congrus à 3 (mod 4) prennent en compte progressivement les nombres de base, chaque facteur premier congru à 1 (mod 4) doit prendre en compte l'ensemble des contraintes imposées par chacun des nombres de base. Chaque facteur premier congru à 1 (mod 4), soit p, de p_{f-e} à p_f, doit avoir passé avec succès l'examen suivant en deux étapes.

1) **L'étape (1) s'exécute successivement pour chacun des m nombres de base de g_1 à g_m.**

On calcule le symbole de Legendre du nombre de base courant g par rapport au candidat p. Un et un seul des deux cas suivants se présente : Si le symbole vaut –1, on rejette le candidat. Sinon (le symbole vaut +1), on poursuit l'examen en passant au nombre de base g suivant à l'étape (1).

Lorsque le candidat est acceptable pour l'ensemble des m nombres de base, on passe à l'étape (2).

2) L'étape (2) s'exécute successivement pour chacune des m valeurs publiques de G_1 à G_m.

On calcule un entier t tel que $p-1$ est divisible par 2^t mais pas par 2^{t+1}, puis, un entier $s = (p-1+2^t)/2^{t+1}$, de façon à établir une clé $\langle s, p\rangle$. On applique la clé $\langle s, p\rangle$ à la valeur publique courante $G = g^2$ pour obtenir un résultat r, soit : $r \equiv G^s \pmod{p}$. Selon le résultat, un et un seul des deux cas suivants se présente :

a) Si r est égal à g ou à $-g$, alors $u = 0$; on poursuit l'examen du candidat en passant à la valeur publique G suivante à l'étape (2).

b) Sinon, on calcule un nombre u positif, prenant une des valeurs de 1 à $t-2$, en appliquant l'algorithme suivant qui met en œuvre deux variables : jj prenant des valeurs allant de 2 à 2^{t-2} et w initialisée par r, ainsi qu'un nombre entier b obtenu en appliquant une clé $\langle (p-1)/2^t, p\rangle$ à un résidu non quadratique de CG(p).

Pour un indice ii allant de 1 à $t-2$, on répète l'opération suivante :

On calcule $w^2/G \pmod{p}$, puis, on applique une clé $\langle 2^{t-ii-1}, p\rangle$ au résultat pour obtenir +1 ou –1 (sinon, on a une preuve que le candidat n'est pas premier). Si l'on obtient –1, alors on calcule $jj = 2^{ii}$, puis, $c \equiv b^{jj} \pmod{p}$, puis, on remplace w par $w.c \pmod{p}$, puis, on passe à l'indice ii suivant. Si l'on obtient +1, on passe à l'indice ii suivant.

A l'issue de l'algorithme, la valeur figurant dans la variable jj définit u par la relation $jj = 2^{t-u}$; la valeur figurant dans la variable w est une racine carrée de G, c'est-à-dire, g ou $-g$ (sinon, on a une preuve que le

candidat n'est pas premier). Deux cas se présentent :

- Si $t-u < k$, alors on rejette le candidat p parce que la branche où figure G n'est pas assez longue.
- Sinon ($t-u \geq k$), on poursuit l'évaluation du candidat en passant à la valeur publique G suivante à l'étape (2).

Lorsque le candidat est acceptable pour l'ensemble des m valeurs publiques, il est accepté comme facteur premier congru à 1 (mod 4).

Calcul des valeurs associées

Pour obtenir les composantes privées, calculons toutes les solutions à l'équation (3.a) dans les deux cas les plus simples et les plus courants avant d'aborder le cas général.

Pour chaque facteur premier p_j congru à 3 (mod 4), la clé $\langle (p_j+1)/4,\ p_j \rangle$ donne la racine carrée quadratique de n'importe quel résidu quadratique. On en déduit une manière de calculer une solution à l'équation (3.a) :

$$s_j \equiv ((p_j+1)/4)^k \pmod{(p_j-1)/2} ; \quad \text{puis,} \quad Q_{i,j} \equiv G_i^{sj} \pmod{p_j}$$

ou bien plutôt, l'inverse (mod p_j) d'une telle solution.

$$s_j \equiv (p_j-1)/2-((p_j+1)/4)^k \pmod{(p_j-1)/2} ; \quad \text{puis,} \quad Q_{i,j} \equiv G_i^{sj} \pmod{p_j}$$

Dans CG(p_j), il y a alors deux et seulement deux racines carrées de l'unité : +1 et −1 ; il y a donc deux solutions en x à l'équation (3.a) : les deux nombres $Q_{i,j}$ et $p_j-Q_{i,j}$ ont le même carré G_i (mod p_j).

Pour chaque facteur premier p_j congru à 5 (mod 8), la clé $\langle (p_j+3)/8,\ p_j \rangle$ donne la racine carrée de rang impair de n'importe quel élément de rang impair. On en déduit une solution à l'équation (3.a) :

$$s_j \equiv ((p_j+3)/8)^k \pmod{(p_j-1)/4} ; \quad \text{puis,} \quad Q_{i,j} \equiv G_i^{sj} \pmod{p_j}$$

ou bien plutôt, l'inverse (mod p_j) d'une telle solution.

$$s_j \equiv (p_j-1)/4-((p_j+3)/8)^k \pmod{(p_j-1)/4} ; \quad \text{puis,} \quad Q_{i,j} \equiv G_i^{sj} \pmod{p_j}$$

Dans CG(p_j), il y a alors quatre et seulement quatre racines quatrièmes de l'unité ; il y a donc quatre solutions en x à l'équation (3.a). Remarquons que $2^{(pj-1)/4}$ (mod p_j) est une racine carrée de −1 parce que le symbole de Legendre de 2 par rapport à p congru à 5 (mod 8) vaut −1. Si $Q_{i,j}$ est une

solution, alors $p_j - Q_{i,j}$ est une autre solution, ainsi que le produit (mod p_j) de $Q_{i,j}$ par une racine carrée de -1.

Pour un facteur premier p_j congru à 2^t+1 (mod 2^{t+1}), la clé $\langle (p_j-1+2^t)/2^{t+1}, p_j \rangle$ donne la racine carrée de rang impair de n'importe quel élément de rang impair. On peut donc calculer une solution à l'équation (3.a).

- Calculons d'abord un nombre entier $s_j \equiv ((p_j-1+2^t)/2^{t+1})^k \pmod{(p_j-1)/2^t}$ pour établir une clé $\langle s_j, p_j \rangle$.
- Lorsque la clé $\langle (p_j-1+2^t)/2^{t+1}, p_j \rangle$ transforme G_i en g_i ou en $-g_i$, le rang de G_i est impair dans CG(p_j) ($u = 0$). Alors, la clé $\langle s_j, p_j \rangle$ transforme G_i en un nombre z : c'est la solution de rang impair à l'équation (3.a). Selon les valeurs de t et de k, il y a encore $\min(2^k-1, 2^t-1)$ autres solutions sur une ou plusieurs branches. La branche de z^2 porte une autre solution : c'est $p_j - z$. Lorsque $t \geq 2$, la branche de z^4 porte deux autres solutions : c'est le produit de z par chacune des deux racines carrées de -1, c'est-à-dire, chacune des deux racines quatrièmes primitives de l'unité. Or, si y est un résidu non quadratique de CG(p_j), alors, $y^{(pj-1)/4} \pmod{p_j}$ est une racine carrée de -1. D'une manière générale, pour i prenant chaque valeur de 1 à $\min(k, t)$, la branche de la puissance 2^i ième de z porte 2^{i-1} solutions : ce sont les produits (mod p_j) de z par chacune des 2^{i-1} racines 2^i ièmes primitives de l'unité. Or, si y est un résidu non quadratique de CG(p_j), alors, y à la puissance $(p_j-1)/2^i$ est une racine 2^i ième primitive de l'unité que nous nommons c. Les 2^{i-1} racines 2^i ièmes primitives de l'unité sont les puissances impaires de c : c, $c^3 \pmod{p_j}$, $c^5 \pmod{p_j}$, ... c à la puissance $2^i-1 \pmod{p_j}$.
- Lorsque la clé $\langle (p_j-1+2^t)/2^{t+1}, p_j \rangle$ transforme G_i en un nombre entier r qui n'est ni g_i ni $-g_i$, le rang de G_i est pair dans CG(p_j) ($u > 0$). Alors, à condition que G_i soit convenablement placé sur une branche assez longue, c'est-à-dire, $t \geq k + u$, il y a 2^k solutions sur la branche où figure G_i. Pour calculer une racine 2^k ième, il suffit de réitérer k fois de rang l'algorithme de calcul de racine carrée donné ci-dessus, de façon à

calculer les racines carrées des résultats successifs jusqu'à une solution z. Ce calcul peut bien sûr être optimisé pour approcher directement une racine 2^k ième et ajuster ensuite une seule fois l'approximation d'une racine 2^k ième pour atteindre une solution z. Pour obtenir toutes les autres solutions, remarquons tout d'abord que si y est un résidu non quadratique de CG(p_j), alors, y à la puissance $(p_j-1)/2^k$ est une racine 2^k ième primitive de l'unité que nous nommons d. Les 2^k racines 2^k ièmes de l'unité sont les puissances successives de d : d, d^2 (mod p_j), d^3 (mod p_j), ... d à la puissance 2^k-1 (mod p_j), d à la puissance 2^k (mod p_j) qui vaut 1. Les 2^k solutions sur la branche où figure G_i sont les produits (mod p_j) de z par chacune de ces racines.

En résumé, pour calculer une composante pour le facteur premier p et le nombre de base g, connaissant k, t et u, on procède comme suit :

1) On calcule un nombre entier : $s \equiv ((p-1+2^t)/2^{t+1})^k$ (mod $(p-1)/2^t$) pour établir une clé $\langle s, p\rangle$. Puis, on applique la clé $\langle s, p\rangle$ à G pour obtenir $z \equiv G^s$ (mod p). Selon la valeur de u, on passe à l'étape (2) ou (3).
2) Si $u = 0$, z est la solution de rang impair à l'équation (3.a). Il y a encore $\min(2^k-1, 2^t-1)$ autres solutions de rang pair sur une ou plusieurs branches, très exactement sur $\min(k, t)$ autres branches. Pour i allant de 1 à $\min(k, t)$, la branche de la puissance 2^i ième de z porte 2^{i-1} solutions : ce sont les produits (mod p) de z par chacune des 2^{i-1} racines 2^i ièmes primitives de l'unité. La solution générique à l'équation (3.a) est représentée par zz. On passe à l'étape (4).
3) Si $u > 0$, toutes les solutions à l'équation (3.a) sont de rang pair. Il y en a 2^k et elles figurent toutes sur la branche où figure G ; en effet : $t-u \geq k$. Pour calculer une solution, l'algorithme suivant met en œuvre deux variables : jj prenant des valeurs allant de 2 à 2^{t-2} et w initialisée par z, ainsi qu'un nombre entier b obtenu en appliquant une clé $\langle (p-1)/2^t, p\rangle$ à un résidu non quadratique de CG(p).

On répète k fois de rang la séquence suivante :

Pour un indice *ii* allant de 1 à t–2, on répète l'opération suivante : On calcule w^2/G (mod p), puis, on applique une clé $\langle 2^{t-ii-1}, p\rangle$ au résultat pour obtenir +1 ou –1 (sinon, on a une preuve que p n'est pas premier). Si l'on obtient –1, alors on calcule $jj = 2^{ii}$, puis, $c \equiv b^{jj}$ (mod p), puis, on remplace w par $w.c$ (mod p), puis, on passe à l'indice *ii* suivant. Si l'on obtient +1, on passe à l'indice *ii* suivant.

A l'issue de l'algorithme, la variable w a pour valeur za. Les 2^k solutions sur la branche où figure G sont les produits (mod p) de za par chacune des 2^k racines 2^k ièmes de l'unité. La solution générique à l'équation (3.a) est représentée par zz. On passe à l'étape (4).

4) Connaissant zz, on en déduit une valeur de composante : c'est l'inverse de zz modulo p lorsque l'équation $G.Q^v \equiv 1$ (mod n) est utilisée et zz lorsque l'équation $G \equiv Q^v$ (mod n) est utilisée.

Remarque. Il y a diverses méthodes pour obtenir les composantes privées et les valeurs privées. Connaissant une collection de f composantes, c'est-à-dire, les f composante pour un nombre de base donné, la technique des restes chinois permet de calculer la valeur privée correspondante. On voit ainsi que, pour une valeur publique G et un module n donnés, il peut y avoir plusieurs valeurs privées Q possibles. Il y en a quatre lorsque n est le produit de deux facteurs premiers congrus à 3 (mod 4) ; il y en a huit avec trois facteurs premiers congrus à 3 (mod 4) ; il y en a seize avec deux facteurs premiers congrus à 3 (mod 4) et un congru à 5 (mod 8). Un usage judicieux de ces multiples valeurs peut compliquer les attaques par analyse de la consommation électrique d'une carte à puce utilisant GQ2.

Ainsi, au fur et à mesure que t augmente, le programme se complique pour des cas de plus en plus rares. En effet, les nombres premiers se répartissent en moyenne comme suit : $t = 1$ pour un sur deux, $t = 2$ pour un sur quatre, $t = 3$ pour un sur huit, et ainsi de suite. De plus, les contraintes dues aux m nombres de base rendent les candidatures de moins en moins acceptables. Quoi qu'il en soit, les modules mixtes font définitivement partie de la

technologie GQ2 ; le type du module GQ2 n'affecte en rien les protocoles d'authentification dynamique et de signature numérique.

La figure 3 illustre $G_i = g_i^2$ sur un cycle avec un facteur premier p congru à 9 (mod 16), c'est-à-dire, $t = 3$, $u = 0$, ainsi que $k \geq 3$. On peut noter que :

$$b \equiv y^{\frac{p-1}{8}} \pmod{p}$$

$$b^8 \equiv 1 \pmod{p}$$

$$b^4 \equiv -1 \pmod{p}$$

La figure 4 illustre $G_i = g_i^2$ sur une branche avec un facteur premier p congru à 65 (mod 128), c'est-à-dire, $t = 6$, ainsi que $k = 4$ et $u = 2$.

Voici un premier jeu de clés GQ2 avec $\boldsymbol{k = 6}$, soit $v = 64$, $\boldsymbol{m = 3}$, soit trois nombres de base : $g_1 = 3$, $g_2 = 5$ et $g_3 = 7$, et $\boldsymbol{f = 3}$, soit un module à trois facteurs premiers : deux congrus à 3 (mod 4) et un à 5 (mod 8). Notons que $g = 2$ est incompatible avec un facteur premier congru à 5 (mod 8).

p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833

$(2 \mid p_1) = -1$; $(3 \mid p_1) = +1$; $(5 \mid p_1) = -1$; $(7 \mid p_1) = +1$

p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B

$(2 \mid p_1) = -1$; $(3 \mid p_1) = -1$; $(5 \mid p_1) = +1$; $(7 \mid p_1) = -1$

p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD

$(2 \mid p_1) = -1$; $(3 \mid p_1) = +1$; $(5 \mid p_1) = +1$; $(7 \mid p_1) = +1$

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9
02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144
CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD

$Q_{1,1}$ = 0279C60D216696CD6F7526E23512DAE090CFF879FDDE

$Q_{2,1}$ = 7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89

$Q_{3,1}$ = 6FB3B9C05A03D7CADA9A3425571EF5ECC54D7A7B6F

$Q_{1,2}$ = 0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502

$Q_{2,2}$ = 04792CE70284D16E9A158C688A7B3FEAF9C40056469E

$Q_{3,2}$ = FDC4A8E53E185A4BA793E93BEE5C636DA731BDCA4E

$Q_{1,3}$ = 07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE

$Q_{2,3}$ = 0AE8551E116A3AC089566DFDB3AE003CF174FC4E4877

$Q_{3,3}$ = 01682D490041913A4EA5B80D16B685E4A6DD88070501

Q_1 = D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8
C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A
C74D9743435AB4D7CF0FF6557

Q_2 = CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4
DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8
82288273ADE67353A5BC316C093

Q_3 = 09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A
AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197
697238537FE7A0195C5E8373EB74D

Voici d'autres valeurs possibles pour les composantes liées au facteur p_3 lequel est congru à 5 (mod 8).

Voici une racine carrée de –1 dans CG(p_3) : $c = 2^{(p3-1)/4} \pmod{p_3}$ =
0C3000933A854E4CB309213F12CAD59FA7AD775AAC37

$Q'_{1,3} = c \,.\, Q_{1,3} \pmod{p_3}$ =
050616671372B87DEC9AEEAC68A3948E9562F714D76C

$Q'_{2,3} = c \,.\, Q_{2,3} \pmod{p_3}$ =
06F308B529C9CE88D037D01002E7C838439DACC9F8AA

$Q'_{3,3} = c \,.\, Q_{3,3} \pmod{p_3}$ =
015BE9F4B92F1950A69766069F788E45439497463D58

Ce qui donne :

Q'_1 = 676DF1BA369FF306F4A1001602BCE5A008DB82882E87C148D0
D820A711121961C9376CB45C355945C5F2A9E5AFAAD7861886284A
9B319F9E4665211252D74580

Q'_2 = CAEC4F41752A228CF9B23B16B3921E47C059B9E0C68634C2C
64D6003156F30EF1BC02ADA25581C8FDE76AA14AB5CC60A2DE1C
565560B27E8AA0E6F4BCA7FE966

Q'_3 = 2ACDF5161FE53B68CC7C18B6AFE495815B46599F44C51A6A1
A4E858B470E8E5C7D2200EF135239AF0B7230388A6A5BDD8EE15B
0D094FC2BFA890BFDA669D9735

Voici un second jeu de clés GQ2, avec $k = 9$, soit $v = 512$, $m = 2$, soit deux nombres de base : $g_1 = 2$ et $g_2 = 3$, et $f = 3$, soit un module à trois facteurs premiers congrus à 3 (mod 4).

p_1 = 03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB

$(2 \mid p_1) = -1$; $(3 \mid p_1) = -1$; et on trouve bien, $(6 \mid p_1) = +1$.

p_2 = 062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7

$(2 \mid p_2) = +1$; $(3 \mid p_2) = -1$; et on trouve bien, $(6 \mid p_2) = -1$.

p_3 = 0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3

$(2 \mid p_3) = -1$; $(3 \mid p_3) = +1$; et on trouve bien, $(6 \mid p_3) = -1$.

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D
6698AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49
761B276A8E6B6977A21D51669D039F1D7

$Q_{1,1}$ = 0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1

$Q_{2,1}$ = 0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E

$Q_{1,2}$ = 02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A

$Q_{2,2}$ = 045ECB881387582E7C556887784D2671CA118E22FCF2

$Q_{1,3}$ = B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982

$Q_{2,3}$ = 0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB

Q_1 = 27F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C
35F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6
EDDA092D0CF108D0AB708405DA46

Q_2 = 230D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64
9C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6
F11F19874DE7DC5D1DF2A9252D

Dans la présente demande, on a décrit un procédé pour produire des jeux de clés GQ2, à savoir, des modules n et des couples de valeurs publique G et privée Q dans le cas où l'exposant v est égal à 2^k. Ces jeux de clés sont utilisés pour mettre en œuvre un procédé destiné à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message ainsi que cela a été décrit.

ANNEXE 2

Procédé, système, dispositif destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

La présente invention concerne les procédés, les systèmes ainsi que les dispositifs destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Le brevet EP 0 311 470 B1 dont les inventeurs sont Louis Guillou et Jean-Jacques Quisquater décrit un tel procédé. On y fera ci-après référence en le désignant par les termes : "brevet GQ" ou "procédé GQ". Par la suite on désignera parfois par "GQ2", "invention GQ2" ou "technologie GQ2" la présente invention.

Selon le procédé GQ, une entité appelée " autorité de confiance " attribue une identité à chaque entité appelée " témoin" et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : "*Voici mon identité ; j'en connais la signature RSA.*" Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant le procédé GQ se déroulent "sans transfert de connaissance". Selon le procédé GQ, le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Le procédé GQ met en œuvre des calculs modulo des nombres de 512 bits ou davantage. Ces calculs concernent des nombres ayant sensiblement la même taille élevés à des puissances de l'ordre de $2^{16} + 1$. Or les infrastructures microélectroniques existantes, notamment dans le domaine des cartes bancaires, font usage de microprocesseurs auto-programmables monolithiques dépourvus de coprocesseurs arithmétiques. La charge de

travail liée aux multiples opérations arithmétiques impliquées par des procédés tels que le procédé GQ, entraîne des temps de calcul qui dans certains cas s'avèrent pénalisant pour les consommateurs utilisant des cartes bancaires pour acquitter leurs achats. Il est rappelé ici, qu'en cherchant à accroître la sécurité des cartes de paiement, les autorités bancaires posent un problème particulièrement délicat à résoudre. En effet, il faut traiter deux questions apparemment contradictoires : augmenter la sécurité en utilisant des clés de plus en plus longues et distinctes pour chaque carte tout en évitant que la charge de travail n'entraîne des temps de calcul prohibitifs pour les utilisateurs. Ce problème prend un relief particulier dans la mesure où, en outre, il convient de tenir compte de l'infrastructure en place et des composants microprocesseurs existants.

La technologie GQ précédemment décrite fait appel à la technologie RSA. Mais si la technologie RSA dépend bel et bien de la factorisation du module n, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites "multiplicatives" contre les diverses normes de signature numérique mettant en oeuvre la technologie RSA.

L'objectif de la technologie GQ2 est double : d'une part, améliorer les performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La connaissance de la clé privée GQ2 est équivalente à la connaissance de la factorisation du module n. Toute attaque au niveau des triplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 évite les inconvénients présentés par la technologie RSA.

Procédé

Méthode des restes chinois appliquée à la famille GQ

Plus particulièrement, l'invention concerne un procédé destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n \ ;$$

Ledit procédé met en œuvre selon les étapes ci-après définies une entité appelée témoin disposant des **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et de l'exposant public **v** .

Le témoin calcule des engagements **R** dans l'anneau des entiers modulo **n.** Chaque engagement est calculé en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$, puis en appliquant la méthode des restes chinois,

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des engagements R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le témoin reçoit un ou plusieurs défis **d**. Chaque défi **d** comportant **m**

entiers $\mathbf{d_i}$ ci-après appelés défis élémentaires. Le témoin calcule à partir de chaque défi **d** une réponse **D**, en effectuant des opérations du type :

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{\ d1} \cdot Q_{i,2}^{\ d2} \cdot \ldots Q_{i,m}^{\ dm} \bmod p_i}$$

puis en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo $\mathbf{p_i}$ à effectuer pour calculer chacune des réponses $\mathbf{D_i}$ pour chacun des $\mathbf{p_i}$ est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le procédé est tel qu'il y a autant de réponses **D** que de défis **d** que d'engagements **R**, chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le procédé selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur. Ladite entité démonstrateur comprend le témoin. Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

- **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le démonstrateur transmet au contrôleur tout ou partie de chaque engagement **R.**

- **étape 2 : acte de défi d**

Le contrôleur, après avoir reçu tout ou partie de chaque engagement **R,** produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** au démonstrateur.

- **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Le démonstrateur transmet chaque réponse **D** au contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque

engagement R

Dans le cas où le démonstrateur a transmis une partie de chaque engagement **R,** le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Le contrôleur vérifie que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** qui lui a été transmis.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement **R,** le contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifie que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Cas de la preuve de l'intégrité d'un message

dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le procédé selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ladite entité démonstrateur comprend le témoin.

Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

- **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus.

- **étape 2 : acte de défi d**

Le démonstrateur applique une fonction de hachage **h** ayant comme

arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**. Le démonstrateur transmet le jeton **T** au contrôleur. Le contrôleur, après avoir reçu un jeton **T**, produit des défis **d** en nombre égal au nombre d'engagements **R** et transmet les défis **d** a u démonstrateur.

- **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Le démonstrateur transmet chaque réponse **D** au contrôleur Le contrôleur, disposant des m valeurs publiques $G_1, G_2, \ldots G_m$, calcule à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n.$$

Puis, le contrôleur applique la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**. Puis, le contrôleur vérifie que le jeton **T'** est identique au jeton **T** transmis.

Signature numérique d'un message et preuve de son authenticité

Opération de signature

Dans une troisième variante de réalisation susceptible d'être prise en combinaison avec l'une et/ou l'autre des autres variantes de réalisation, le procédé selon l'invention est destiné à produire la signature numérique d'un message **M** par une entité appelée entité signataire. Ladite entité signataire comprend le témoin.

Ladite entité signataire exécute une opération de signature en vue d'obtenir un message signé comprenant :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D**.

Ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, le témoin calcule chaque engagement **R** en appliquant le processus spécifié ci-dessus.

- **étape 2 : acte de défi d**

Le signataire applique une fonction de hachage **h** ayant comme arguments le message **M** et chaque engagement **R** pour obtenir un train binaire. Le signataire extrait de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R.**

- **étape 3 : acte de réponse D**

Le témoin calcule des réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

Opération de contrôle

Pour l'authenticité du message **M,** une entité, appelée contrôleur, contrôle le message signé. Ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme ci-après décrit.

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

Dans le cas où le contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,** le contrôleur vérifie que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n}$$

Puis, le contrôleur vérifie que le message **M,** les défis **d** et les engagements

R satisfont à la fonction de hachage

$$\mathbf{d = h\ (M, R)}$$

• cas où le contrôleur dispose des défis d et des réponses D

Dans le cas où le contrôleur dispose des défis **d** et des réponses **D,** le contrôleur reconstruit, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} .\ \bmod n}$$

Puis, le contrôleur vérifie que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h\ (M, R')}$$

• cas où le contrôleur dispose des engagements R et des réponses D

Dans le cas où le contrôleur dispose des engagements **R** et des réponses **D,** le contrôleur applique la fonction de hachage et reconstruit **d'**

$$\mathbf{d' = h\ (M, R)}$$

Puis, le contrôleur vérifie que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$\mathbf{R \equiv G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d'1} . G_2^{\,d'2} . \ldots G_m^{\,d'm} .\ \bmod n.}$$

Cas où on choisit la valeur privée Q en premier et où on déduit la valeur publique G de la valeur privée Q

Dans certains, notamment afin de faciliter la production des couples de valeurs privées **Q** et publiques **G**, on choisit la valeur privée **Q** en premier et on déduit la valeur publique **G** de la valeur privée **Q.** Plus particulièrement dans ce cas, le procédé selon l'invention est tel que les composantes $Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$ des valeurs privées Q_i, sont des nombres tirés au hasard à raison d'une composante $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) pour

chacun desdits facteurs premiers p_j. Lesdites valeurs privées Q_i peuvent être calculées à partir desdites composantes $Q_{i,1}$, $Q_{i,2}$ ... $Q_{i,f}$ par la méthode des restes chinois. Lesdites valeurs publiques G_i, sont calculées en effectuant des opérations du type

$$G_{i,j} \equiv Q_{i,j}^{\ v} \bmod p_j$$

puis, en appliquant la méthode des restes chinois pour établir G_i tel que

$$G_i \,.\, Q_i^{\ v} \equiv 1 \,.\, \bmod n \text{ ou } G_i \equiv Q_i^{\ v} \bmod n \ ;$$

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des $G_{i,j}$ pour chacun des p_j est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo **n**.

Avantageusement dans ce cas, le proc d selon l'invention l exposant public de v rification v est un nombre premier. la s curit est quivalente la connaissance de la valeur Cas o on choisit la valeur publique G en premier et o on valeur priv e Q de la valeur publique G.

De préférence dans ce cas, ledit exposant **v** est tel que

$$v = {}^{k}2$$

o k est un param tre de s curit plus grand que 1 .

Ladite valeur publique G est un nombre de base inférieur auxf facteurs premiers p_f . Le nombre de base tel que les deux quations :

$$x^2 \equiv g_i \bmod n \qquad \text{et} \qquad x^2 \equiv - g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n** et tel que l'équation :

$$x^v \equiv g_i^{\,2} \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n**.

Système

La présente invention concerne également un système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs étant liés par des relations du type :

$$G_i \,.\, Q_i^{\,v} \equiv 1 \,.\, \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^{\,v} \,\mathbf{mod}\ n \,.$$

Ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif témoin comporte une zone mémoire contenant les **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \,\mathbf{mod}\ p_j$) des valeurs privées Q_i et de l'exposant public **v.** Le dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,
- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin, pour calculer des engagements **R** dans l'anneau des entiers modulo **n.** Chaque engagement est calculé en effectuant des opérations du type

$$R_i \equiv r_i^{\,v} \,\mathbf{mod}\ p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo $\mathbf{p_i}$ à effectuer pour calculer chacun des engagements $\mathbf{R_i}$ pour chacun des $\mathbf{p_i}$ est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers $\mathbf{d_i}$ ci-après appelés défis élémentaires ;

- des moyens de calcul, ci-après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

puis, en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Ledit dispositif témoin comporte aussi des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D.** Il y a autant de réponses **D** que de défis **d** que d'engagements **R.** Chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le système selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système comporte aussi un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur. Ledit système permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désigné les moyens de transmission du dispositif démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion.

- **étape 2 : acte de défi d**

Le dispositif contrôleur comporte des moyens de productions de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R,** des défis **d** en nombre égal au nombre d'engagements **R.** Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

- **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin

calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur. Le dispositif contrôleur comporte aussi

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement **R,** les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu.

cas où le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement **R,** les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbf{mod\ n} .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le système selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit système comporte aussi un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur.

Ledit système exécute les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion.

- **étape 2 : acte de défi d**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif démonstrateur, appliquant une

fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre chaque jeton **T** , via les moyens de connexion, au dispositif au contrôleur. Le dispositif contrôleur comporte aussi des moyens de productions de défis pour produire, après avoir reçu le jeton **T,** des défis **d** en nombre égal au nombre d'engagements **R,** Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

- **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au contrôleur. Le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement

reconstruit **R'**, un jeton **T'**.

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton **T'** au jeton **T** reçu.

Signature numérique d'un message et preuve de son authenticité

Opération de signature

Dans une troisième variante de réalisation, susceptible d'être combinée à l'une et/ou à l'autre des deux autres, le système selon l'invention est destiné à produire la signature numérique d'un message **M**, ci après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponses **D** .

Ledit système est tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au dispositif témoin par des moyens d'interconnexion et peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion.

• **étape 2 : acte de défi d**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction d hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R.**

• **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif signataire, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

Opération de contrôle

Pour prouver l'authenticité du message **M**, par une entité appelée contrôleur, contrôle le message signé.

Le système comporte un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur.

Ledit dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion. Ainsi, le dispositif contrôleur dispose d'un message signé comprenant:

- le message **M**,

- les défis **d** et/ou les engagements **R**,

- les réponse **D**.

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

Dans le cas où le dispositif contrôleur dispose des engagements **R**, des défis **d**, des réponses **D**, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M**, les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\,(M, R)}$$

• cas où le contrôleur dispose des défis d et des réponses D

Dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D**, les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \ldots G_m^{\,dm} . \bmod n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifie

que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h\ (M, R')}$$

• cas où le contrôleur dispose des engagements R et des réponses D

Dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D,** les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$\mathbf{d' = h\ (M, R)}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$\mathbf{R \equiv G_1}^{\mathbf{d'1}} \mathbf{. G_2}^{\mathbf{d'2}} \mathbf{. \ldots G_m}^{\mathbf{d'm}} \mathbf{. D^v\ mod\ n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1}^{\mathbf{d'1}} \mathbf{. G_2}^{\mathbf{d'2}} \mathbf{. \ldots G_m}^{\mathbf{d'm}} \mathbf{.\ mod\ n}$$

Cas où on choisit la valeur privée Q en premier et où on déduit la valeur publique G de la valeur privée Q

Dans certains, notamment afin de faciliter la production des couples de valeurs privées **Q** et publiques **G**, on choisit la valeur privée **Q** en premier et on déduit la valeur publique **G** de la valeur privée **Q.** Plus particulièrement dans ce cas, le système selon l'invention est tel que les composantes $\mathbf{Q_{i,1}}$, $\mathbf{Q_{i,2}}$, ... $\mathbf{Q_{i,f}}$ des valeurs privées $\mathbf{Q_i}$, sont des nombres tirés au hasard à raison d'une composante $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i\ mod\ p_j}$) pour chacun desdits facteurs premiers $\mathbf{p_j}$. Lesdites valeurs privées $\mathbf{Q_i}$ peuvent être calculées à partir desdites composantes $\mathbf{Q_{i,1}}$, $\mathbf{Q_{i,2}}$ ... $\mathbf{Q_{i,f}}$ par la méthode des restes chinois. Lesdites valeurs publiques $\mathbf{G_i}$, sont calculées en effectuant des opérations du type

$$\mathbf{G_{i,j} \equiv\ Q_{i,j}^v\ mod\ p_j}$$

puis, en appliquant la méthode des restes chinois pour établir $\mathbf{G_i}$ tel que

$$\mathbf{G_i . Q_i^v \equiv 1\ .\ mod\ n}\ \text{ou}\ \mathbf{G_i \equiv Q_i^v\ mod\ n}\ ;$$

Ainsi, le nombre d'opérations arithmétiques modulo $\mathbf{p_i}$ à effectuer pour

calculer chacun des $G_{i,j}$ pour chacun des p_j est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo **n**.

Avantageusement dans ce cas, le système selon l'invention l'exposant public de vérification v est un nombre premier. La sécurité est équivalente à la connaissance de la valeur Cas où on choisit la valeur publique G en premier et on détermine la valeur privée Q de la valeur publique G.

De préférence dans ce cas, ledit exposant **v** est tel que

$$v = {}^{k}2$$

où k est un paramètre de sécurité plus grand que 1. Ladite G_i est le carré d'un nombre g_i inférieur aux facteurs premiers p_1, p_2 p_f. Le nombre g_i choisi tel que les deux équations :

$$x^2 \equiv g_i \bmod n \qquad \text{et} \qquad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo **n** et tel que l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo **n** .

Dispositif terminal

Méthode des restes chinois appliquée à la famille GQ

L'invention concerne aussi un dispositif terminal associé à une entité. Le dispositif terminal se présente notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif terminal est destiné à prouver à dispositif contrôleur :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées Q_1, Q_2, ... Q_m et publiques G_1, G_2, ... G_m (**m** étant supérieur ou égal à 1),

- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),

- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n .$$

Ledit dispositif terminal comprend un dispositif témoin comportant une zone mémoire contenant les **f** facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou les **m** valeurs privées Q_i et/ou les **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs privées Q_i et de l'exposant public **v.** Le dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements **R** du dispositif témoin.

Les moyens de calcul permettent de calculer des engagements **R** dans l'anneau des entiers modulo **n.** Chaque engagement est calculé en effectuant des opérations du type

$$R_i \equiv r_i^v \mathbf{mod}\ p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des engagements R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis **d** du dispositif témoin, pour recevoir un ou plusieurs défis **d**,

chaque défi **d** comportant **m** entiers $\mathbf{d_i}$ ci-après appelés défis élémentaires ;

- des moyens de calcul, ci-après désignés les moyens de calcul des réponses **D** du dispositif témoin, pour calculer à partir de chaque défi **d** une réponse **D** en effectuant des opérations du type :

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}}^{\mathbf{d1}} \mathbf{\cdot Q_{i,2}}^{\mathbf{d2}} \mathbf{\cdot \ldots Q_{i,m}}^{\mathbf{dm}} \mathbf{\bmod p_i}$$

puis, en appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo $\mathbf{p_i}$ à effectuer pour calculer chacune des réponses $\mathbf{D_i}$ pour chacun des $\mathbf{p_i}$ est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n.

Le dispositif témoin comporte aussi des moyens de transmission pour transmettre un ou plusieurs engagements **R** et une ou plusieurs réponses **D.** Il y a autant de réponses **D** que de défis **d** que d'engagements **R.** Chaque groupe de nombres **R, d, D** constituant un triplet noté **{R, d, D}.**

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation, le dispositif terminal selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif terminal est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit dispositif démonstrateur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement **R** au dispositif contrôleur, via les moyens de connexion.

- **étape 2 et 3 : acte de défi d, acte de réponse D**

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque défi **d** provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation, susceptible d'être combinée aux autres variantes de réalisation, le dispositif terminal selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message **M** associé à une entité appelée démonstrateur. Ledit dispositif terminal est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des

moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit dispositif démonstrateur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif démonstrateur, via les moyens d'interconnexion.

- **étape 2 et 3 : acte de défi d, acte de réponse**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif démonstrateur, appliquant fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer au moins un jeton **T**. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre chaque jeton **T** , via les moyens de connexion, au dispositif au contrôleur.

Ledit dispositif contrôleur produit, après avoir reçu le jeton **T**, des défis **d** en nombre égal au nombre d'engagements **R**.

Les moyens de réception des défis **d** du dispositif témoin, reçoivent chaque

défi **d** provenant du dispositif démonstrateur, via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse **D** au dispositif contrôleur qui procède au contrôle.

Signature numérique d'un message et preuve de son authenticité

Opération de signature

Dans une troisième variante de réalisation, susceptible d'être combinée aux autres, le dispositif terminal selon l'invention est destiné à produire la signature numérique d'un message **M,** ci après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- le message **M,**
- les défis **d** et/ou les engagements **R,**
- les réponses **D.**

Ledit dispositif terminal étant tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit dispositif signataire comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

• **étape 1 : acte d'engagement R**

A chaque appel, les moyens de calcul des engagements **R** du dispositif témoin calculent chaque engagement **R** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement **R** au dispositif signataire, via les moyens d'interconnexion.

• **étape 2 : acte de défi d**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction d hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement **R** pour calculer un train binaire et extraire de ce train binaire des défis **d** en nombre égal au nombre d'engagements **R.**

• **étape 3 : acte de réponse D**

Les moyens de réception des défis **d** reçoivent les défis **d** provenant du dispositif signataire, via les moyens d'interconnexion. Les moyens de calcul des réponses **D** du dispositif témoin calculent les réponses **D** à partir des défis **d** en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses **D** au dispositif signataire, via les moyens d'interconnexion.

Dispositif contrôleur

Méthode des restes chinois appliquée à toute la famille GQ

L'invention concerne aussi un dispositif contrôleur. Le dispositif contrôleur peut se présenter notamment sous la forme d'un terminal ou d'un serveur distant associé à une entité contrôleur. Le dispositif contrôleur est destiné à prouver à un serveur contrôleur :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message **M** associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (**m** étant supérieur ou égal à 1),
- un module public **n** constitué par le produit de **f** facteurs premiers $p_1, p_2, \ldots p_f$ (**f** étant supérieur ou égal à 2),
- un exposant public **v** .

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \ . \ \mathbf{mod\ n} \text{ ou } G_i \equiv Q_i^v \ \mathbf{mod\ n} \ ;$$

où Q_i désigne une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i .

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation, susceptible d'être combinée avec les autres, le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associé à l'entité démonstrateur.

Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

- **étape 1 et 2 : acte d'engagement R, acte de défi**

Ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements **R** provenant du dispositif démonstrateur, via les moyens de connexion.

Le dispositif contrôleur comporte des moyens de productions de défis pour produire, après avoir reçu tout ou partie de chaque engagement **R**, des défis **d** en nombre égal au nombre d'engagements **R**, chaque défi **d** comportant

m entiers d_i , ci-après appelés défis élémentaires.

Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

- **étapes 3 et 4 : acte de réponse, acte de contrôle**

Le dispositif contrôleur comporte aussi

- des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion,

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement R

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement **R,** les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, calculent à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot D^v \bmod n$$

ou à une relation du type,

$$R' \equiv D^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n \,.$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit **R'** à tout ou partie de chaque engagement **R** reçu.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement R

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus l'intégralité de chaque engagement **R,** les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des **m** valeurs publiques

$G_1, G_2, \ldots G_m$, vérifient que chaque engagement **R** satisfait à une relation du type :

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type,

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation, susceptible d'être combinée avec les autres, le dispositif contrôleur selon l'invention est destiné à prouver l'intégrité d'un message **M** associé à une entité appelée démonstrateur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associé à l'entité démonstrateur.

Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

- **étapes 1 et 2 : acte d'engagement R, acte de défi**

Ledit dispositif contrôleur comporte aussi des moyens de réception de jetons **T** provenant du démonstrateur, via les moyens de connexion. Le dispositif contrôleur comporte aussi des moyens de productions de défis pour produire, après avoir reçu le jeton **T,** défis **d** en nombre égal au nombre d'engagements **R** , chaque défi **d** comportant **m** entiers, ci-après appelés les défis élémentaires. Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif contrôleur, pour transmettre les défis **d** au démonstrateur, via les moyens de connexion.

- **étapes 3 et 4 : acte de réponse D, acte de contrôle**

Le dispositif contrôleur comporte des moyens de réception des réponses **D** provenant du dispositif démonstrateur, via les moyens de connexion. Le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés

les moyens de calcul du dispositif contrôleur, disposant des **m** valeurs publiques G_1, G_2, ... G_m, pour d'une part, calculer à partir de chaque défi **d** et de chaque réponse **D** un engagement reconstruit **R'** satisfaisant à une relation du type :

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

ou à une relation du type :

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

puis d'autre part, calculer en appliquant la fonction de hachage **h** ayant comme arguments le message **M** et tout ou partie de chaque engagement reconstruit **R'**, un jeton **T'**.

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton **T'** au jeton **T** reçu.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation, susceptible d'être combinée aux autres variantes de réalisation, le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité du message **M** en contrôlant, par une entité appelée contrôleur, le message signé.

Le message signé, émis par un dispositif signataire associé à une entité signataire disposant d'une fonction de hachage **h (M, R)** ; comprend :

- le message **M**,
- les défis **d** et/ou les engagements **R**,
- les réponse **D** .

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif signataire associé à l'entité signataire. Ledit dispositif contrôleur reçoit le message signé du dispositif signataire, via les moyens de connexion.

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

• cas où le contrôleur dispose des engagements R, des défis d, des réponses D,

Dans le cas où le dispositif contrôleur dispose des engagements **R,** des défis **d,** des réponses **D,** les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d** et les réponses **D** satisfont à des relations du type

$$\mathbf{R \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R \equiv D^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M,** les défis **d** et les engagements **R** satisfont à la fonction de hachage

$$\mathbf{d = h\,(M, R)}$$

• cas où le contrôleur dispose des défis d et des réponses D

Dans le cas où le dispositif contrôleur dispose des défis **d** et des réponses **D,** les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi **d** et de chaque réponse **D**, des engagements **R'** satisfaisant à des relations du type :

$$\mathbf{R' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot D^v \bmod n}$$

ou à des relations du type :

$$\mathbf{R' \equiv D^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message **M** et les défis **d** satisfont à la fonction de hachage

$$\mathbf{d = h\,(M, R')}$$

• cas où le contrôleur dispose des engagements R et des réponses D

Dans le cas où le dispositif contrôleur dispose des engagements **R** et des réponses **D,** les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent **d'** tel que

$$d' = h\,(M, R)$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements **R**, les défis **d'** et les réponses **D**, satisfont à des relations du type :

$$R \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot D^v \bmod n$$

ou à des relations du type :

$$R \equiv D^v / G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \bmod n$$

Description d taill e de la variante de r alisation da l exposant public v = 2^k

Description

Rappelons l'objectif de la technologie GQ : l'authentification dynamique d'entités et de messages associés, ainsi que la signature numérique de messages.

La version classique de la technologie GQ fait appel à la technologie RSA. Mais, si la technologie RSA dépend bel et bien de la factorisation, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites « multiplicatives » contre diverses normes de signature numérique mettant en œuvre la technologie RSA.

Dans le cadre de la technologie GQ2, la présente partie de l'invention porte plus précisément sur l'utilisation des jeux de clés GQ2 dans le cadre de l'authentification dynamique et de la signature numérique. La technologie GQ2 ne fait pas appel à la technologie RSA. L'objectif est double : d'une part, améliorer les performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La clé privée GQ2 est la factorisation du module n. Toute attaque au niveau de striplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 concurrence la technologie RSA.

La technologie GQ2 utilise un ou plusieurs petits nombres entiers plus grands que 1, disons m petits nombres entiers ($m \geq 1$) appelés « nombres de base » et notés par g_i. Les nombres de base étant fixés de g_1 à g_m avec $m \geq 1$, une clé publique de vérification $\langle v, n \rangle$ est choisie de la manière suivante. L'exposant public de vérification v est 2^k où k est un petit nombre entier plus grand que 1 ($k \geq 2$). Le module public n est le produit d'au moins deux facteurs premiers plus grands que les nombres de base, disons f facteurs premiers ($f \geq 2$) notés par p_j, de $p_1 \ldots p_f$. Les f facteurs premiers

sont choisis de façon à ce que le module public n ait les propriétés suivantes par rapport à chacun des m nombres de base de g_1 à g_m.

- D'une part, les équations (1) et (2) n'ont pas de solution en x dans l'anneau des entiers modulo n, c'est-à-dire que g_i et $-g_i$ sont deux résidus non quadratiques (mod n).

$$x^2 \equiv g_i \pmod{n} \qquad (1)$$

$$x^2 \equiv -g_i \pmod{n} \qquad (2)$$

- D'autre part, l'équation (3) a des solutions en x dans l'anneau des entiers modulo n.

$$x^{2^k} \equiv g_i^2 \pmod{n} \qquad (3)$$

La clé publique de vérification $\langle v, n \rangle$ étant fixée selon les nombres de base de g_1 à g_m avec $m \geq 1$, chaque nombre de base g_i détermine un couple de valeurs GQ2 comprenant une valeur publique G_i et une valeur privée Q_i : soit m couples notés de G_1 Q_1 à G_m Q_m. La valeur publique G_i est le carré du nombre de base g_i : soit $G_i = g_i^2$. La valeur privée Q_i est une des solutions à l'équation (3) ou bien l'inverse (mod n) d'une telle solution.

De même que le module n se décompose en f facteurs premiers, l'anneau des entiers modulo n se décompose en f corps de Galois, de CG(p_1) à CG(p_f). Voici les projections des équations (1), (2) et (3) dans CG(p_j).

$$x^2 \equiv g_i \pmod{p_j} \qquad (1.a)$$

$$x^2 \equiv -g_i \pmod{p_j} \qquad (2.a)$$

$$x^{2^k} \equiv g_i^2 \pmod{p_j} \qquad (3.a)$$

Chaque valeur privée Q_i peut se représenter de manière unique par f composantes privées, une par facteur premier : $Q_{i,j} \equiv Q_i \pmod{p_j}$. Chaque composante privée $Q_{i,j}$ est une solution à l'équation (3.a) ou bien l'inverse (mod p_j) d'une telle solution. Après que toutes les solutions possibles à chaque équation (3.a) aient été calculées, la technique des restes chinois permet d'établir toutes les valeurs possibles pour chaque valeur privée Q_i à partir de f composantes de $Q_{i,1}$ à $Q_{i,f}$: Q_i = Restes Chinois ($Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$)

de manière à obtenir toutes les solutions possibles à l'équation (3).

Voici la technique des restes chinois : soient deux nombres entiers positifs premiers entre eux a et b tels que $0 < a < b$, et deux composantes X_a de 0 à $a-1$ et X_b de 0 à $b-1$; il s'agit de déterminer X = Restes Chinois (X_a, X_b), c'est-à-dire, le nombre unique X de 0 à $a.b-1$ tel que $X_a \equiv X \pmod{a}$ et $X_b \equiv X \pmod{b}$. Voici le paramètre des restes chinois : $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$. Voici l'opération des restes chinois : $\varepsilon \equiv X_b \pmod{a}$; $\delta = X_a - \varepsilon$; si δ est négatif, remplacer δ par $\delta + a$; $\gamma \equiv \alpha . \delta \pmod{a}$; $X = \gamma . b + X_b$.

Lorsque les facteurs premiers sont rangés dans l'ordre croissant, du plus petit p_1 au plus grand p_f, les paramètres des restes chinois peuvent être les suivants (il y en a $f-1$, c'est-à-dire, un de moins que de facteurs premiers). Le premier paramètre des restes chinois est $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$. Le second paramètre des restes chinois est $\beta \equiv \{p_1.p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$. Le i ième paramètre des restes chinois est $\lambda \equiv \{p_1.p_2. \ldots p_{i\_1} \pmod{p_i}\}^{-1} \pmod{p_i}$. Et ainsi de suite. Ensuite, en $f-1$ opérations des restes chinois, on établit un premier résultat (mod p_2 fois p_1) avec le premier paramètre, puis, un second résultat (mod $p_1.p_2$ fois p_3) avec le second paramètre, et ainsi de suite, jusqu'à un résultat (mod $p_1. \ldots p_{f\_1}$ fois p_f), c'est-à-dire, (mod n).

Il y a plusieurs représentations possibles de la clé privée GQ2, ce qui traduit **le polymorphisme de la clé privée GQ2**. Les diverses représentations s'avèrent équivalentes : elles se ramènent toutes à la connaissance de la factorisation du module n qui est la véritable clé privée GQ2. Si la représentation affecte bien le comportement de l'entité qui signe ou qui s'authentifie, elle n'affecte pas le comportement de l'entité qui contrôle.

Voici les trois principales représentations possibles de la clé privée GQ2. 1) La représentation classique en technologie GQ consiste à stocker m valeurs privées Q_i et la clé publique de vérification $\langle v, n \rangle$; en technologie GQ2, cette représentation est concurrencée par les deux suivantes. 2) La représentation optimale en termes de charges de travail consiste à stocker

l'exposant public v, les f facteurs premiers p_j, $m.f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois. 3) La représentation optimale en termes de taille de clé privée consiste à stocker l'exposant public v, les m nombres de base g_i et les f facteurs premiers p_j, puis, à commencer chaque utilisation en établissant ou bien m valeurs privées Q_i et le module n pour se ramener à la première représentation, ou bien $m.f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois pour se ramener à la seconde.

Les entités qui signent ou s'authentifient peuvent toutes utiliser les mêmes nombres de base ; sauf contre indication, les m nombres de base de g_1 à g_m peuvent alors avantageusement être les m premiers nombres premiers.

Parce que la sécurité du mécanisme d'authentification dynamique ou de signature numérique équivaut à la connaissance d'une décomposition du module, la technologie GQ2 ne permet pas de distinguer simplement deux entités utilisant le même module. Généralement, chaque entité qui s'authentifie ou signe dispose de son propre module GQ2. Toutefois, on peut spécifier des modules GQ2 à quatre facteurs premiers dont deux sont connus d'une entité et les deux autres d'une autre.

Voici un premier jeu de clés GQ2 avec $\boldsymbol{k = 6}$, soit $v = 64$, $\boldsymbol{m = 3}$, soit trois nombres de base : $g_1 = 3$, $g_2 = 5$ et $g_3 = 7$, et $\boldsymbol{f = 3}$, soit un module à trois facteurs premiers : deux congrus à 3 (mod 4) et un à 5 (mod 8). Notons que $g = 2$ est incompatible avec un facteur premier congru à 5 (mod 8).

p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833

p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B

p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD

$n = p_1 . p_2 . p_3$ = FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9
02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144
CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD

$Q_{1,1}$ = 0279C60D216696CD6F7526E23512DAE090CFF879FDDE

$Q_{2,1}$ = 7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89

$Q_{3,1}$ = 6FB3B9C05A03D7CADA9A3425571EF5ECC54D7A7B6F

$Q_{1,2}$ = 0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502

$Q_{2,2}$ = 04792CE70284D16E9A158C688A7B3FEAF9C40056469E

$Q_{3,2}$ = FDC4A8E53E185A4BA793E93BEE5C636DA731BDCA4E

$Q_{1,3}$ = 07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE

$Q_{2,3}$ = 0AE8551E116A3AC089566DFDB3AE003CF174FC4E4877

$Q_{3,3}$ = 01682D490041913A4EA5B80D16B685E4A6DD88070501

Q_1 = D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8
C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A
C74D9743435AB4D7CF0FF6557

Q_2 = CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4
DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8
82288273ADE67353A5BC316C093

Q_3 = 09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A
AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197
697238537FE7A0195C5E8373EB74D

Voici un second jeu de clés GQ2, avec $k = 9$, soit $v = 512$, $m = 2$, soit deux nombres de base : $g_1 = 2$ et $g_2 = 3$, et $f = 3$, soit un module à trois facteurs premiers congrus à 3 (mod 4).

p_1 = 03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB

p_2 = 062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7

p_3 = 0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D
6698AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49
761B276A8E6B6977A21D51669D039F1D7

$Q_{1,1}$ = 0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1

$Q_{2,1}$ = 0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E

$Q_{1,2}$ = 02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A

$Q_{2,2}$ = 045ECB881387582E7C556887784D2671CA118E22FCF2

$Q_{1,3}$ = B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982

$Q_{2,3}$ = 0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB

Q_1 = 27F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C
35F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6
EDDA092D0CF108D0AB708405DA46

Q_2 = 230D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64
9C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6
F11F19874DE7DC5D1DF2A9252D

Authentification dynamique

Le mécanisme d'authentification dynamique est destiné à prouver à une entité appelée **contrôleur** l'authenticité d'une autre entité appelée **démonstrateur** ainsi que l'authenticité d'un éventuel message associé *M*, de sorte que le contrôleur s'assure qu'il s'agit bien du démonstrateur et éventuellement que lui et le démonstrateur parlent bien du même message *M*. Le message associé *M* est optionnel, ce qui signifie qu'il peut être vide.

Le mécanisme d'authentification dynamique est une séquence de quatre actes : un acte d'engagement, un acte de défi, un acte de réponse et un acte de contrôle. Le démonstrateur joue les actes d'engagement et de réponse. Le contrôleur joue les actes de défi et de contrôle.

Au sein du démonstrateur, on peut isoler un témoin, de manière à isoler les paramètres et les fonctions les plus sensibles du démonstrateur, c'est-à-dire, la production des engagements et des réponses. Le témoin dispose du paramètre *k* et de la clé privée GQ2, c'est-à-dire, de la factorisation du module *n* selon l'une des trois représentations évoquées ci-dessus : • les *f* facteurs premiers et les *m* nombres de base, • les *m.f* composantes privées, les *f* facteurs premiers et *f*–1 paramètres des restes chinois, • les *m* valeurs privées et le module *n*.

Le témoin peut correspondre à une réalisation particulière, par exemple, • une carte à puce reliée à un PC formant ensemble le démonstrateur, ou

encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce. Le témoin ainsi isolé est semblable au témoin défini ci-après au sein du signataire. A chaque exécution du mécanisme, le témoin produit un ou plusieurs engagements R, puis, autant de réponses D à autant de défis d. Chaque ensemble $\{R, d, D\}$ constitue un **triplet GQ2**.

Outre qu'il comprend le témoin, le démonstrateur dispose également, le cas échéant, d'une fonction de hachage et d'un message M.

Le contrôleur dispose du module n et des paramètres k et m ; le cas échéant, il dispose également de la même fonction de hachage et d'un message M'. Le contrôleur est apte à reconstituer un engagement R' à partir de n'importe quel défi d et de n'importe quelle réponse D. Les paramètres k et m renseignent le contrôleur. Faute d'indication contraire, les m nombres de base de g_1 à g_m sont les m premiers nombres premiers. Chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m : un par nombre de base. Chaque défi élémentaire de d_1 à d_m doit prendre une valeur de 0 à $2^{k-1}-1$ (les valeurs de $v/2$ à $v-1$ ne sont pas utilisées). Typiquement, chaque défi est codé par m fois $k-1$ bits (et non pas m fois k bits). Par exemple, avec $k = 6$ et $m = 3$ et les nombres de base 3, 5 et 7, chaque défi comporte 15 bits transmis sur deux octets ; avec $k = 9$, $m = 2$ et les nombres de base 2 et 3, chaque défi comporte 16 bits transmis sur deux octets. Lorsque les $(k-1).m$ défis possibles sont également probables, la valeur $(k-1).m$ détermine la sécurité apportée par chaque triplet GQ2 : un imposteur qui, par définition, ne connaît pas la factorisation du module n a exactement une chance de succès sur $2^{(k-1).m}$. Lorsque $(k-1).m$ vaut de 15 à 20, un triplet suffit à assurer raisonnablement l'authentification dynamique. Pour atteindre n'importe quel niveau de sécurité, on peut produire des triplets en parallèle ; on peut également en produire en séquence, c'est-à-dire, répéter l'exécution du mécanisme.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Voici un exemple avec le premier jeu de clés avec $k = 6$.

r = B8AD426C1AC0165E94B894AC2437C1B1797EF562CFA53A4AF8
43131FF1C89CFDA131207194710EF9C010E8F09C60D9815121981260
919967C3E2FB4B4566088E

R = FFDD736B666F41FB771776D9D50DB7CDF03F3D976471B25C56
D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C21210C6B04
49CC4292E5DD2BDB00828AF18

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i), il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Voici un exemple avec le second jeu de clés avec $k = 9$.

r_1 = B0418EABEBADF0553A28903F74472CD49EE8C82D86

R_1 = 022B365F0BEA8E157E94A9DEB0512827FFD5149880F1

r_2 = 75A8DA8FE0E60BD55D28A218E31347732339F1D667

R_2 = 057E43A242C485FC20DEEF291C774CF1B30F0163DEC2

r_3 = 0D74D2BDA5302CF8BE2F6D406249D148C6960A7D27

R_3 = 06E14C8FC4DD312BA3B475F1F40CF01ACE2A88D5BB3C

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

R = Restes Chinois(R_1, R_2, ... R_f)

R = 28AA7F12259BFBA81368EB49C93EEAB3F3EC6BF73B0EBD7
D3FC8395CFA1AD7FC0F9DAC169A4F6F1C46FB4C3458D1E37C9
9123B56446F6C928736B17B4BA4A529

Dans les deux cas, le démonstrateur transmet au contrôleur tout ou partie de chaque engagement ***R***, ou bien, un code de hachage ***H*** obtenu en hachant chaque engagement ***R*** et un message ***M***.

2) L'acte de défi consiste à tirer au hasard un ou plusieurs défis d composés chacun de m défis élémentaires d_1 d_2 ... d_m ; chaque défi élémentaire d_i prend l'une des valeurs de 0 à $v/2-1$.

$$d = d_1\ d_2 \ldots\ d_m$$

Voici un exemple pour le premier jeu de clés avec $k = 6$ et $m = 3$.

$$d_1 = 10110 = 22 = \text{'16'}\ ;\ d_2 = 00111 = 7\ ;\ d_3 = 00010 = 2,$$

$$d = 0\ ||\ d_1\ ||\ d_2\ ||\ d_3 = 01011000\ 11100010 = 58\ E2$$

Voici un exemple pour le second jeu de clés avec $k = 9$ et $m = 2$.

$$d = d_1\ ||\ d_2 = 58\ E2 = \text{soit en décimal, 88 et 226}$$

Le contrôleur transmet au démonstrateur chaque défi ***d***.

3) L'acte de réponse comporte les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les valeurs privées selon les défis élémentaires.

$$X \equiv Q_1^{d_1}\ Q_2^{d_2} \cdot Q_m^{d_m} \pmod{n}$$

$$D \equiv rX \pmod{n}$$

Voici un exemple pour le premier jeu de clés.

D = FF257422ECD3C7A03706B9A7B28EE3FC3A4E974AEDCDF386
5EEF38760B859FDB5333E904BBDD37B097A989F69085FE8EF6480
A2C6A290273479FEC9171990A17

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il calcule une ou plusieurs collections de f

composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$X_i \equiv Q_{1,i}^{d_1} Q_{2,i}^{d_2} \cdot Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i X_i \pmod{p_i}$$

Voici un exemple pour le second jeu de clés.

$D_1 = r_1 \cdot Q_{1,1}^{d1} \cdot Q_{2,1}^{d2} \pmod{p_1} =$
02660ADF3C73B6DC15E196152322DDE8EB5B35775E38

$D_2 = r_2 \cdot Q_{1,2}^{d1} \cdot Q_{2,2}^{d2} \pmod{p_2} =$
04C15028E5FD1175724376C11BE77052205F7C62AE3B

$D_3 = r_3 \cdot Q_{1,3}^{d1} \cdot Q_{2,3}^{d2} \pmod{p_3} =$
0903D20D0C306C8EDA9D8FB5B3BEB55E061AB39CCF52

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

D = 85C3B00296426E97897F73C7DC6341FB8FFE6E879AE12EF1F36
4CBB55BC44DEC437208CF530F8402BD9C511F5FB3B3A309257A00
195A7305C6FF3323F72DC1AB

Dans les deux cas, le démonstrateur transmet chaque réponse $\boldsymbol{D}$ au contrôleur.

4) L'acte de contrôle consiste à contrôler que chaque triplet $\{R, d, D\}$ vérifie une équation du type suivant pour une valeur non nulle,

$$R \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

ou bien, à rétablir chaque engagement : aucun ne doit être nul.

$$R \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Eventuellement, le contrôleur calcule ensuite un code de hachage H' en

hachant chaque engagement rétabli R' et un message M'. L'authentification dynamique est réussie lorsque le contrôleur retrouve ainsi ce qu'il a reçu à l'issue de l'acte d'engagement, c'est-à-dire, tout ou partie de chaque engagement R, ou bien, le code de hachage H.

Par exemple, une séquence d'opérations élémentaires transforme la réponse D en un engagement R'. La séquence comprend k carrés (mod n) séparés par k–1 divisions ou multiplications (mod n) par des nombres de base. Pour la i ième division ou multiplication, qui s'effectue entre le i ième carré et le i+1 ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, ... jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m.

Voici un exemple pour le premier jeu de clés.

D^2 (mod n) =

FD12E8E1F1370AEC9C7BA2E05C80AD2B692D341D46F3
2B93948715491F0EB091B7606CA1E744E0688367D7BB998F7B73D5F7
FDA95D5BD6347DC8B978CA217733

3 . D^2 (mod n) = F739B708911166DFE715800D8A9D78FC3F332FF622D
3EAB8E7977C68AD44962BEE4DAE3C0345D1CB34526D3B67EBE8BF
987041B4852890D83FC6B48D3EF6A9DF

3^2 . D^4 (mod n) = 682A7AF280C49FE230BEE354BF6FFB30B7519E3C8
92DD07E5A781225BBD33920E5ADABBCD7284966D71141EAA17AF
8826635790743EA7D9A15A33ACC7491D4A7

3^4 . D^8 (mod n) = BE9D828989A2C184E34BA8FE0F384811642B7B548F
870699E7869F8ED851FC3DB3830B2400C516511A0C28AFDD210EC3
939E69D413F0BABC6DEC441974B1A291

3^5 . 5 . D^8 (mod n) = 2B40122E225CD858B26D27B768632923F2BBE5
DB15CA9EFA77EFA667E554A02AD1A1E4F6B59BD9E1AE4A537D
4AC1E89C2235C363830EBF4DB42CEA3DA98CFE00

3^{10} . 5^2 . D^{16} (mod n) =

BDD3B34C90ABBC870C604E27E7F2E9DB2D383
68EA46C931C66F6C7509B118E3C162811A98169C30D4DEF768397DD
B8F6526B6714218DEB627E11FACA4B9DB268

$3^{11} \cdot 5^{3} \cdot 7 \cdot D^{16} \pmod{n} =$
DBFA7F40D338DE4FBA73D42DBF427BBF195
C13D02AB0FA5F8C8DDB5025E34282311CEF80BACDCE5D0C433444
A2AF2B15318C36FE2AE02F3C8CB25637C9AD712F

$3^{22} \cdot 5^{6} \cdot 7^{2} \cdot D^{32} \pmod{n}$ = C60CA9C4A11F8AA89D9242CE717E3DC6C1
A95D5D09A2278F8FEE1DFD94EE84D09D000EA8633B53C4A0E7F0A
EECB70509667A3CB052029C94EDF27611FAE286A7

$3^{22} \cdot 5^{7} \cdot 7^{2} \cdot D^{32} \pmod{n} =$
DE40CB6B41C01E722E4F312AE7205F18CDD
0303EA52261CB0EA9F0C7E0CD5EC53D42E5CB645B6BB1A3B00C77
886F4AC5222F9C863DACA440CF5F1A8E374807AC

$3^{44} \cdot 5^{14} \cdot 7^{4} \cdot D^{64} \pmod{n}$, c'est-à-dire, $3^{2C} \cdot 5^{E} \cdot 7^{4} \cdot D^{40} \pmod{n}$ avec les exposants en hexa = FFDD736B666F41FB771776D9D50DB7CDF03F3D9
76471B25C56D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C
21210C6B0449CC4292E5DD2BDB00828AF18

On retrouve bien l'engagement ***R***. L'authentification est réussie.

Voici un exemple pour le second jeu de clés.

$D^{2} \pmod{n}$ = C66E585D8F132F7067617BC6D00BA699ABD74FB9D13E
24E6A6692CC8D2FC7B57352D66D34F5273C13F20E3FAA228D70AEC
693F8395ACEF9206B172A8A2C2CCBB

$3 \cdot D^{2} \pmod{n}$ = 534C6114D385C3E15355233C5B00D09C2490D1B8D8E
D3D59213CB83EAD41C309A187519E5F501C4A45C37EB2FF38FBF20
1D6D138F3999FC1D06A2B2647D48283

$3^{2} \cdot D^{4} \pmod{n}$ = A9DC8DEA867697E76B4C18527DFFC49F4658473D03
4EC1DDE0EB21F6F65978BE477C4231AC9B1EBD93D5D49422408E47
15919023B16BC3C6C46A92BBD326AADF

$2 \cdot 3^3 \cdot D^4 \pmod{n}$ = FB2D57796039DFC4AF9199CAD44B66F257A1FF
3F2BA4C12B0A8496A0148B4DFBAFE838E0B5A7D9FB4394379D72A
107E45C51FCDB7462D03A35002D29823A2BB5
$2^2 \cdot 3^6 \cdot D^8 \pmod{n}$ = 4C210F96FF6C77541910623B1E49533206DFB9E91
6521F305F12C5DB054D4E1BF3A37FA293854DF02B49283B6DE5E5D
82ACB23DAF1A0D5A721A1890D03A00BD8
$2^2 \cdot 3^7 \cdot D^8 \pmod{n}$ = E4632EC4FE4565FC4B3126B15ADBF996149F2D
BB42F65D911D3851910FE7EA53DAEA7EE7BA8FE9D081DB78B249
B1B18880616B90D4E280F564E49B270AE02388
$2^4 \cdot 3^{14} \cdot D^{16} \pmod{n}$ = ED3DDC716AE3D1EA74C5AF935DE814BCC
2C78B12A6BB29FA542F9981C5D954F53D153B9F0198BA82690EF
665C17C399607DEA54E218C2C01A890D422EDA16FA3
$2^5 \cdot 3^{14} \cdot D^{16} \pmod{n}$ =
DA7C64E0E8EDBE9CF823B71AB13F17E1161487
6B000FBB473F5FCBF5A5D8D26C7B2A05D03BDDD588164E562D0F5
7AE94AE0AD3F35C61C0892F4C91DC0B08ED6F
$2^{10} \cdot 3^{28} \cdot D^{32} \pmod{n}$ = 6ED6AFC5A87D2DD117B0D89072C99FB9DC9
5D558F65B6A1967E6207D4ADBBA32001D3828A35069B256A07C3D
722F17DA30088E6E739FBC419FD7282D16CD6542
$2^{11} \cdot 3^{28} \cdot D^{32} \pmod{n}$ = DDAD5F8B50FA5BA22F61B120E5933F73B92
BAAB1ECB6D432CFCC40FA95B77464003A705146A0D364AD40F8
7AE45E2FB460111CDCE73F78833FAE505A2D9ACA84
$2^{22} \cdot 3^{56} \cdot D^{64} \pmod{n}$ = A466D0CB17614EFD961000BD9EABF4F021
36F8307101882BC1764DBAACB715EFBF5D8309AE001EB5DEDA
8F000E44B3D4578E5CA55797FD4BD1F8E919BE787BD0
$2^{44} \cdot 3^{112} \cdot D^{128} \pmod{n}$ = 925B0EDF5047EFEC5AFABDC03A830919761
B8FBDD2BF934E2A8A31E29B976274D513007EF1269E4638B4F65F
8FDEC740778BDC178AD7AF2968689B930D5A2359
$2^{44} \cdot 3^{113} \cdot D^{128} \pmod{n}$ = B711D89C03FDEA8D1F889134A4F809B3F2D

8207F2AD8213D169F2E99ECEC4FE08038900F0C203B55EE4F4C803
BFB912A04F11D9DB9D076021764BC4F57D47834

$2^{88} \cdot 3^{226} \cdot D^{256} \pmod{n} =$
41A83F119FFE4A2F4AC7E5597A5D0BEB4D4C
08D19E597FD034FE720235894363A19D6BC5AF323D24B1B7FCFD8D
FCC628021B4648D7EF757A3E461EF0CFF0EA13

$2^{176} \cdot 3^{452} \cdot D^{512} \pmod{n}$, soit $4^{88} \cdot 9^{226} \cdot D^{512} \pmod{n} =$
28AA7F12259BFBA8
1368EB49C93EEAB3F3EC6BF73B0EBD7D3FC8395CFA1AD7FC0F9D
AC169A4F6F1C46FB4C3458D1E37C99123B56446F6C928736B17B4BA
4A529

On retrouve bien l'engagement *R*. L'authentification est réussie.

Signature numérique

Le mécanisme de signature numérique permet à une entité appelée **signataire** de produire des messages signés et à une entité appelée **contrôleur** de vérifier des messages signés. Le message *M* est une séquence binaire quelconque : il peut être vide. Le message *M* est signé en lui adjoignant un appendice de signature qui comprend un ou plusieurs engagements et / ou défis, ainsi que les réponses correspondantes.

Le contrôleur dispose de la même fonction de hachage, des paramètres k et m et du module n. Les paramètres ***k*** et ***m*** renseignent le contrôleur. D'une part, chaque défi élémentaire, de d_1 à d_m, doit prendre une valeur de 0 à $2^{k-1}-1$ (les valeurs de $v/2$ à $v-1$ ne sont pas utilisées). D'autre part, chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m, autant que de nombres de base. En outre, faute d'indication contraire, les m nombres de base, de g_1 à g_m, sont les m premiers nombres premiers. Avec $(k-1).m$ valant de 15 à 20, on peut signer avec quatre triplets GQ2 produits en parallèle ; avec $(k-1).m$ valant 60 ou plus, on peut signer avec un seul triplet GQ2. Par exemple, avec $k = 9$ et $m = 8$, un seul triplet GQ2 suffit ; chaque défi

comporte huit octets et les nombres de base sont 2, 3, 5, 7, 11, 13, 17 et 19.

L'opération de signature est une séquence de trois actes : un acte d'engagement, un acte de défi et un acte de réponse. Chaque acte produit un ou plusieurs triplets GQ2 comprenant chacun : un engagement R ($\neq 0$), un défi d composé de m défis élémentaires notés par d_1, d_2, ... d_m et une réponse D ($\neq 0$).

Le signataire dispose d'une fonction de hachage, du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. **Au sein du signataire, on peut isoler un témoin qui exécute les actes d'engagement et de réponse**, de manière à isoler les fonctions et les paramètres les plus sensibles du démonstrateur. Pour calculer engagements et réponses, le témoin dispose du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. Le témoin ainsi isolé est semblable au témoin défini au sein du démonstrateur. Il peut correspondre à une réalisation particulière, par exemple, • une carte à puce reliée à un PC formant ensemble le signataire, ou encore, • des programmes particulièrement protégés au sein d'un PC, ou encore, • des programmes particulièrement protégés au sein d'une carte à puce.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i),

il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

$$R = \text{Restes Chinois}(R_1, R_2, \ldots R_f)$$

2) L'acte de défi consiste à hacher tous les engagements R et le message à signer M pour obtenir un code de hachage à partir duquel le signataire forme un ou plusieurs défis comprenant chacun m défis élémentaires ; chaque défi élémentaire prend une valeur de 0 à $v/2-1$; par exemple, avec $k = 9$ et $m = 8$, chaque défi comporte huit octets. Il y a autant de défis que d'engagements.

$$d = d_1\ d_2 \ldots\ d_m, \text{ extraits du résultat Hash}(M, R)$$

3) L'acte de réponse comporte les opérations suivantes.

Lorsque la témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les valeurs privées selon les défis élémentaires.

$$X \equiv Q_1^{d_1} Q_2^{d_2} \cdot Q_m^{d_m} \pmod{n}$$

$$D \equiv rX \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il calcule une ou plusieurs collections de f composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$X_i \equiv Q_{1,i}^{d_1} Q_{2,i}^{d_2} \cdot Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i X_i \pmod{p_i}$$

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

Le signataire signe le message M en lui adjoignant un appendice de signature comprenant :

- ou bien, chaque triplet GQ2, c'est-à-dire, chaque engagement R, chaque défi d et chaque réponse D,
- ou bien, chaque engagement R et chaque réponse D correspondante,
- ou bien, chaque défi d et chaque réponse D correspondante.

Le déroulement de l'opération de vérification dépend du contenu de l'appendice de signature. On distingue les trois cas.

Au cas où l'appendice comprend un ou plusieurs triplets, l'opération de contrôle comporte deux processus indépendants dont la chronologie est indifférente. Le contrôleur accepte le message signé si et seulement si les deux conditions suivantes sont remplies.

D'une part, chaque triplet doit être cohérent (une relation appropriée du type suivant doit être vérifiée) et recevable (la comparaison doit se faire sur une valeur non nulle).

$$R \cdot \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \cdot \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Par exemple, on transforme la réponse D par une séquence d'opérations élémentaires : k carrés (mod n) séparés par $k-1$ multiplications ou divisions (mod n) par des nombres de base. Pour la i ième multiplication ou division, qui s'effectue entre le i ième carré et le $i+1$ ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, ... jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m. On doit ainsi retrouver chaque engagement R présent dans l'appendice de signature.

D'autre part, le ou les triplets doivent être liés au message M. En hachant tous les engagements R et le message M, on obtient un code de hachage à partir duquel on doit retrouver chaque défi d.

$d = d_1\ d_2 \ldots\ d_m$, identiques à ceux extraits du résultat Hash(M, R)

Au cas où l'appendice ne comprend pas de défi, l'opération de contrôle commence par la reconstitution de un ou plusieurs défis d' en hachant tous les engagements R et le message M.

$d' = d'_1\ d'_2 \ldots\ d'_m$, extraits du résultat Hash(M, R)

Ensuite, le contrôleur accepte le message signé si et seulement si chaque triplet est cohérent (une relation appropriée du type suivant est vérifiée) et recevable (la comparaison se fait sur une valeur non nulle).

$$R \prod_{i=1}^{m} G_i^{d'_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \prod_{i=1}^{m} G_i^{d'_i} \pmod{n}$$

Au cas où l'appendice ne comprend pas d'engagement, l'opération de contrôle commence par la reconstitution de un ou plusieurs engagements R' selon une des deux formules suivantes, celle qui est appropriée. Aucun engagement rétabli ne doit être nul.

$$R \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Ensuite, le contrôleur doit hacher tous les engagements R' et le message M de façon à reconstituer chaque défis d.

$d = d_1\ d_2 \ldots\ d_m$, identiques à ceux extraits du résultat Hash(M, R')

Le contrôleur accepte le message signé si et seulement si chaque défi reconstitué est identique au défi correspondant figurant en appendice.

Dans la présente demande, on a montré qu'il existait des couples de valeurs privée Q et publique G permettant de mettre en œuvre le procédé, le système et le dispositif selon l'invention destiné à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Dans la demande pendante déposée le même jour que la présente demande

par France Télécom, TDF et la Société Math RiZK et ayant pour inventeurs Louis Guillou et Jean-Jacques Quisquater, on a décrit un procédé pour produire des jeux de clés GQ2, à savoir, des modules n et des couples de valeurs publique G et privée Q dans le cas où l'exposant v est égal à 2^k. Elle est incorporée ici par référence.

Cette description détaillée de l'invention dans le cas où $v = 2^k$ est susceptible d'être généralisée à d'autres valeurs de v. C'est d'ailleurs ce qui a été exposé, en contrepoint aux revendications, dans les premières pages de la description concernant le cas où v est différent de 2^k. Pour autant que cela soit nécessaire, notamment pour des raisons ressortant des règles d'écriture d'une demande de brevet, et qu'il faille également dans cette partie de la description expliciter l'invention dans le cas où v est différent de 2^k, les premières pages de la description seront également supposées avoir été insérées à la suite de ce paragraphe.

ANNEXE 3

Procédé destiné à prouver l'authenticité d'une entité ou l'intégrité d'un message au moyen d'un exposant public égal à une puissance de deux.

La présente invention concerne les procédés, les systèmes ainsi que les dispositifs destinés à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Le brevet EP 0 311 470 B1 dont les inventeurs sont Louis Guillou et Jean-Jacques Quisquater décrit un tel procédé. On y fera ci-après référence en le désignant par les termes : "brevet GQ" ou " procédé GQ". Par la suite on désignera parfois par "GQ2", "invention GQ2" ou "technologie GQ2" la présente invention.

Selon le procédé GQ, une entité appelée " autorité de confiance " attribue une identité à chaque entité appelée " témoin " et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : " *Voici mon identité ; j'en connais la signature RSA.* " Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée " contrôleur " vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant le procédé GQ se déroulent " sans transfert de connaissance ". Selon le procédé GQ, le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

La technologie GQ précédemment décrite fait appel à la technologie RSA. Mais si la technologie RSA dépend bel et bien de la factorisation du module n, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites "multiplicatives" contre les diverses normes de signature numérique mettant en oeuvre la technologie RSA.

L'objectif de la technologie GQ2 est double : d'une part, améliorer les

performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La connaissance de la clé privée GQ2 est équivalente à la connaissance de la factorisation du module n. Toute attaque au niveau des triplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 évite les inconvénients présentés par la technologie RSA.

Le procédé GQ met en œuvre des calculs modulo des nombres de 512 bits ou davantage. Ces calculs concernent des nombres ayant sensiblement la même taille élevés à des puissances de l'ordre de $2^{16} + 1$. Or les infrastructures microélectroniques existantes, notamment dans le domaine des cartes bancaires, font usage de microprocesseurs auto-programmables monolithiques dépourvus de coprocesseurs arithmétiques. La charge de travail liée aux multiples opérations arithmétiques impliquées par des procédés tels que le procédé GQ, entraîne des temps de calcul qui dans certains cas s'avèrent pénalisant pour les consommateurs utilisant des cartes bancaires pour acquitter leurs achats. Il est rappelé ici, qu'en cherchant à accroître la sécurité des cartes de paiement, les autorités bancaires posent un problème particulièrement délicat à résoudre. En effet, il faut traiter deux questions apparemment contradictoires : augmenter la sécurité en utilisant des clés de plus en plus longues et distinctes pour chaque carte tout en évitant que la charge de travail n'entraîne des temps de calcul prohibitifs pour les utilisateurs. Ce problème prend un relief particulier dans la mesure où, en outre, il convient de tenir compte de l'infrastructure en place et des composants microprocesseurs existants.

La technologie GQ2 a pour objet d'apporter une solution à ce problème tout en renforçant la sécurité.

Procédé

Plus particulièrement, l'invention concerne un procédé destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message $\mathbb{M}$ associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- $\mathbb{m}$ couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ ($\mathbb{m}$ étant supérieur ou égal à 1),
- un module public $\mathbb{n}$ constitué par le produit de $\mathbb{f}$ facteurs premiers $\mathbb{p}_1, \mathbb{p}_2, \ldots \mathbb{p}_f$ ($\mathbb{f}$ étant supérieur ou égal à 2),
- un exposant public $\mathbb{v}$.

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^{\,v} \equiv 1 \ . \bmod n \text{ ou } G_i \equiv Q_i^{\,v} \bmod n$$

Ledit exposant $\mathbb{v}$ est tel que

$$v = 2^k$$

où $\mathbb{k}$ est un paramètre de sécurité plus grand que 1 .

Ladite valeur publique G_i est le carré $g_i^{\,2}$ d'un nombre de base g_i inférieur aux $\mathbb{f}$ facteurs premiers $\mathbb{p}_1, \mathbb{p}_2, \ldots \mathbb{p}_f$. Le nombre de base g_i est tel que :

les deux équations :

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en $\mathbb{x}$ dans l'anneau des entiers modulo $\mathbb{n}$

et tel que :

l'équation :

$$x^v \equiv g_i^{\,2} \bmod n$$

a des solutions en $\mathbb{x}$ dans l'anneau des entiers modulo $\mathbb{n}$.

Ledit procédé met en œuvre selon les étapes ci-après définies une entité appelée témoin. Cette entité dispose des $\mathbb{f}$ facteurs premiers $\mathbb{p}_i$ et/ou des

paramètres des restes chinois des facteurs premiers et/ou du module public n et/ou des m valeurs privées Q_i et/ou des $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et de l'exposant public v .

Le témoin calcule des engagements $\mathbb{R}$ dans l'anneau des entiers modulo n.

Chaque engagement est calculé :

- soit en effectuant des opérations du type

$$\mathbb{R} \equiv r^v \bmod n$$

où r est un aléa tel que $0 < r < n$,

- soit
  - en effectuant des opérations du type

$$\mathbb{R}_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$,

  - puis en appliquant la méthode des restes chinois.

Le témoin reçoit un ou plusieurs défis d. Chaque défi d comporte m entiers d_i ci-après appelés défis élémentaires. Le témoin calcule à partir de chaque défi d une réponse $\mathbb{D}$,

- soit en effectuant des opérations du type :

$$\mathbb{D} \equiv r \cdot Q_1^{\,d1} \cdot Q_2^{\,d2} \cdot \ldots Q_m^{\,dm} \bmod n$$

- soit
  - en effectuant des opérations du type :

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod p_i$$

  - puis en appliquant la méthode des restes chinois.

Ledit procédé est tel qu'il y a autant de réponses $\mathbb{D}$ que de défis d que d'engagements $\mathbb{R}$. Chaque groupe de nombres $\mathbb{R}$, d, $\mathbb{D}$ constitue un triplet noté $\{\mathbb{R}, d, \mathbb{D}\}$.

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le procédé selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une

entité appelée contrôleur. Ladite entité démonstrateur comprend le témoin. Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

- **étape 1 : acte d'engagement $\mathbb{R}$**

A chaque appel, le témoin calcule chaque engagement $\mathbb{R}$ en appliquant le processus spécifié ci-dessus. Le démonstrateur transmet au contrôleur tout ou partie de chaque engagement $\mathbb{R}$.

- **étape 2 : acte de défi d**

Le contrôleur, après avoir reçu tout ou partie de chaque engagement $\mathbb{R}$, produit des défis $\mathbb{d}$ en nombre égal au nombre d'engagements $\mathbb{R}$ et transmet les défis $\mathbb{d}$ au démonstrateur.

- **étape 3 : acte de réponse $\mathbb{D}$**

Le témoin calcule des réponses $\mathbb{D}$ à partir des défis $\mathbb{d}$ en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Le démonstrateur transmet chaque réponse $\mathbb{D}$ au contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement $\mathbb{R}$

Dans le cas où le démonstrateur a transmis une partie de chaque engagement $\mathbb{R}$, le contrôleur, disposant des $\mathbb{m}$ valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque défi $\mathbb{d}$ et de chaque réponse $\mathbb{D}$ un engagement reconstruit $\mathbb{R}'$ satisfaisant à une relation du type :

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

ou a une relation du type,

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n .$$

Le contrôleur vérifie que chaque engagement reconstruit $\mathbb{R}'$ reproduit tout ou partie de chaque engagement $\mathbb{R}$ qui lui a été transmis,

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement $\mathbb{R}$

Dans le cas où le démonstrateur a transmis l'intégralité de chaque engagement $\mathbb{R}$, le contrôleur, disposant des m valeurs publiques G_1, G_2, ... G_m, vérifie que chaque engagement $\mathbb{R}$ satisfait à une relation du type :

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

ou a une relation du type,

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le procédé selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message $\mathbb{M}$ associé à une entité appelée démonstrateur. Ladite entité démonstrateur comprend le témoin.

Lesdites entités démonstrateur et contrôleur exécutent les étapes suivantes:

- **étape 1 : acte d'engagement $\mathbb{R}$**

A chaque appel, le témoin calcule chaque engagement $\mathbb{R}$ en appliquant le processus spécifié ci-dessus.

- **étape 2 : acte de défi d**

Le démonstrateur applique une fonction de hachage h ayant comme arguments le message $\mathbb{M}$ et tout ou partie de chaque engagement $\mathbb{R}$ pour calculer au moins un jeton $\mathbb{T}$. Le démonstrateur transmet le jeton $\mathbb{T}$ au contrôleur. Le contrôleur, après avoir reçu un jeton $\mathbb{T}$, produit des défis d en nombre égal au nombre d'engagements $\mathbb{R}$ et transmet les défis d au démonstrateur.

- **étape 3 : acte de réponse $\mathbb{D}$**

Le témoin calcule des réponses $\mathbb{D}$ à partir des défis d en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Le démonstrateur transmet chaque réponse $\mathbb{D}$ au contrôleur. Le contrôleur, disposant des m valeurs publiques G_1, G_2, ... G_m, calcule à partir de chaque

défi $\mathbb{d}$ et de chaque réponse $\mathbb{D}$ un engagement reconstruit $\mathbb{R}$' satisfaisant à une relation du type :

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

ou à une relation du type :

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Puis le contrôleur applique la fonction de hachage $\mathbb{h}$ ayant comme arguments le message $\mathbb{M}$ et tout ou partie de chaque engagement reconstruit $\mathbb{R}$' pour reconstruire le jeton $\mathbb{T}$'. Puis le contrôleur vérifie que le jeton $\mathbb{T}$' est identique au jeton $\mathbb{T}$ transmis.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée aux deux précédentes, le procédé selon l'invention 1 est destiné à produire la signature numérique d'un message $\mathbb{M}$ par une entité appelée entité signataire. Ladite entité signataire comprend le témoin.

Opération de signature

Ladite entité signataire exécute une opération de signature en vue d'obtenir un message signé comprenant :

- le message $\mathbb{M}$,
- les défis $\mathbb{d}$ et/ou les engagements $\mathbb{R}$,
- les réponses $\mathbb{D}$.

Ladite entité signataire exécute l'opération de signature en mettant en oeuvre les étapes suivantes :

- **étape 1 : acte d'engagement $\mathbb{R}$**

A chaque appel, le témoin calcule chaque engagement $\mathbb{R}$ en appliquant le processus spécifié ci-dessus.

- **étape 2 : acte de défi $\mathbb{d}$**

Le signataire applique une fonction de hachage $\mathbb{h}$ ayant comme arguments le message $\mathbb{M}$ et chaque engagement $\mathbb{R}$ pour obtenir un train binaire. Le signataire extrait de ce train binaire des défis $\mathbb{d}$ en nombre égal au nombre

d'engagements $\mathbb{R}$.

◦ **étape 3 : acte de réponse $\mathbb{D}$**

Le témoin calcule des réponses $\mathbb{D}$ à partir des défis d en appliquant le processus spécifié ci-dessus.

Opération de contrôle

Pour prouver l'authenticité du message $\mathbb{M}$, une entité, appelée contrôleur, contrôle le message signé. Ladite entité contrôleur disposant du message signé exécute une opération de contrôle en procédant comme suit.

◦ **cas où le contrôleur dispose des engagements $\mathbb{R}$, des défis d, des réponses $\mathbb{D}$,**

Dans le cas où le contrôleur dispose des engagements $\mathbb{R}$, des défis d, des réponses $\mathbb{D}$ le contrôleur vérifie que les engagements $\mathbb{R}$, les défis d et les réponses $\mathbb{D}$ satisfont à des relations du type

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

ou à des relations du type :

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Puis le contrôleur vérifie que le message $\mathbb{M}$, les défis d et les engagements $\mathbb{R}$ satisfont à la fonction de hachage

$$d = h(\text{message}, \mathbb{R})$$

◦ **cas où le contrôleur dispose des défis d et des réponses $\mathbb{D}$**

Dans le cas où le contrôleur dispose des défis d et des réponses $\mathbb{D}$, le contrôleur reconstruit, à partir de chaque défi d et de chaque réponse $\mathbb{D}$, des engagements $\mathbb{R}'$ satisfaisant à des relations du type :

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

ou à des relations du type :

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Puis le contrôleur vérifie que le message $\mathbb{M}$ et les défis d satisfont à la fonction de hachage

$$d = h(\text{message}, \mathbb{R}')$$

◦ cas où le contrôleur dispose des engagements $\mathbb{R}$ et des réponses $\mathbb{D}$

Dans le cas où le contrôleur dispose des engagements $\mathbb{R}$ et des réponses $\mathbb{D}$, le contrôleur applique la fonction de hachage et reconstruit d'

$$d' = h\,(\text{message}, \mathbb{R})$$

Puis, contrôleur vérifie que les engagements $\mathbb{R}$, les défis d' et les réponses $\mathbb{D}$, satisfont à des relations du type :

$$\mathbb{R} \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \mathbb{D}^v \bmod n$$

ou à des relations du type :

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \bmod n$$

Système

La présenté invention concerne également un système destiné à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message M associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- m couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ (m étant supérieur ou égal à 1),
- un module public n constitué par le produit de f facteurs premiers $p_1, p_2, \ldots p_f$ (f étant supérieur ou égal à 2),
- un exposant public v ;

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \,.\, \bmod n \text{ ou } G_i \equiv Q_i^v \bmod n \,.$$

Ledit exposant v est tel que

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1 .

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers $p_1, p_2, \ldots p_f$. Le nombre de base g_i est tel que :

les deux équations :

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo n

et tel que :

l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo n .

Ledit système comprend un dispositif témoin, notamment contenu dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif témoin comporte une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et l'exposant public v . Ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements $\mathbb{R}$ du dispositif témoin.

Les moyens de calcul permettent de calculer des engagements $\mathbb{R}$ dans l'anneau des entiers modulo n . Chaque engagement est calculé :

- soit en effectuant des opérations du type

$$\mathbb{R} \equiv r^v \bmod n$$

où r est un aléa produit par les moyens de production d'aléas, r étant tel que $0 < r < n$,

- soit en effectuant des opérations du type

$$\mathbb{R}_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois .

Ledit dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis $\mathbf{d}$ du dispositif témoin, pour recevoir un ou plusieurs défis $\mathbf{d}$; chaque défi $\mathbf{d}$ comportant $\mathbf{m}$ entiers $\mathbf{d_i}$ ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses $\mathbb{D}$ du dispositif témoin, pour calculer à partir de chaque défi $\mathbf{d}$ une réponse $\mathbb{D}$,

  - soit en effectuant des opérations du type :

$$\mathbb{D} \equiv \mathbf{r} \cdot Q_1^{\,d1} \cdot Q_2^{\,d2} \cdot \ldots Q_m^{\,dm} \bmod \mathbf{n}$$

  - soit en effectuant des opérations du type :

$$\mathbb{D}_i \equiv \mathbf{r}_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod \mathbf{p}_i,$$

puis en appliquant la méthode des restes chinois,

Ledit dispositif témoin comporte aussi des moyens de transmission pour transmettre un ou plusieurs engagements $\mathbb{R}$ et une ou plusieurs réponses $\mathbb{D}$. Il y a autant de réponses $\mathbb{D}$ que de défis $\mathbf{d}$ que d'engagements $\mathbb{R}$. Chaque groupe de nombres $\mathbb{R}$, $\mathbf{d}$, $\mathbb{D}$ constitue un triplet noté $\{\mathbb{R}, \mathbf{d}, \mathbb{D}\}$.

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le système selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur,

Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade, par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système comporte aussi un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte

des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur ;

Ledit système permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement $\mathbb{R}$**

A chaque appel, les moyens de calcul des engagements $\mathbb{R}$ du dispositif témoin calculent chaque engagement $\mathbb{R}$ en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement $\mathbb{R}$ au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement $\mathbb{R}$ au dispositif contrôleur, via les moyens de connexion.

- **étape 2 : acte de défi $\mathbb{d}$**

Le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement $\mathbb{R}$, des défis $\mathbb{d}$ en nombre égal au nombre d'engagements $\mathbb{R}$. Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis $\mathbb{d}$ au démonstrateur, via les moyens de connexion.

- **étape 3 : acte de réponse $\mathbb{D}$**

Les moyens de réception des défis $\mathbb{d}$ du dispositif témoin, reçoivent chaque défi $\mathbb{d}$ provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses $\mathbb{D}$ du dispositif témoin, calculent les réponses $\mathbb{D}$ à partir des défis $\mathbb{d}$ en appliquant le processus spécifié ci-dessus.

∘ étape 4 : acte de contrôle

Les moyens de transmission du démonstrateur transmettent chaque réponse $\mathbb{D}$ au contrôleur. Le dispositif contrôleur comporte aussi :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement $\mathbb{R}$

Dans le cas où les moyens de transmission du démonstrateur ont transmis une partie de chaque engagement $\mathbb{R}$, les moyens de calcul du dispositif contrôleur, disposant des m valeurs publiques $G_1, G_2, \ldots G_m$, calculent à partir de chaque défi d et de chaque réponse $\mathbb{D}$ un engagement reconstruit $\mathbb{R}'$ satisfaisant à une relation du type :

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

ou à une relation du type,

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n .$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit $\mathbb{R}'$ à tout ou partie de chaque engagement $\mathbb{R}$ reçu.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement $\mathbb{R}$

Dans le cas où les moyens de transmission du démonstrateur ont transmis l'intégralité de chaque engagement $\mathbb{R}$, les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des m valeurs publiques $G_1, G_2, \ldots G_m$, vérifient que chaque engagement $\mathbb{R}$ satisfait à une relation du type :

$$\mathbb{R} \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

ou à une relation du type,

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n .$$

Cas de la preuve de l'intégrité d'un message.

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le système selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message $\mathbb{M}$ associé à une entité appelée démonstrateur. Ledit système est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Ledit dispositif démonstrateur peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit système comporte aussi dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement; électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif démonstrateur.

Ledit système exécute les étapes suivantes :

- **étape 1 : acte d'engagement $\mathbb{R}$**

A chaque appel, les moyens de calcul des engagements $\mathbb{R}$ du dispositif témoin calculent chaque engagement $\mathbb{R}$ en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement $\mathbb{R}$ au dispositif démonstrateur, via les moyens d'interconnexion.

- **étape 2 : acte de défi d**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage h ayant comme arguments le message $\mathbb{M}$ et tout ou partie de

chaque engagement $\mathbb{R}$, pour calculer au moins un jeton $\mathbb{T}$. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton $\mathbb{T}$, via les moyens de connexion, au dispositif contrôleur. Le dispositif contrôleur comporte aussi des moyens de production de défis pour produire, après avoir reçu le jeton $\mathbb{T}$, des défis $\mathbb{d}$ en nombre égal au nombre d'engagements $\mathbb{R}$. Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis $\mathbb{d}$ au démonstrateur, via les moyens de connexion.

- **étape 3 : acte de réponse $\mathbb{D}$**

Les moyens de réception des défis $\mathbb{d}$ du dispositif témoin, reçoivent chaque défi $\mathbb{d}$ provenant du dispositif démonstrateur, via les moyens d'interconnexion. Les moyens de calcul des réponses $\mathbb{D}$ du dispositif témoin, calculent les réponses $\mathbb{D}$ à partir des défis $\mathbb{d}$ en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse $\mathbb{D}$ au contrôleur. Le dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des $\mathbb{m}$ valeurs publiques $\mathbb{G}_1$, $\mathbb{G}_2$, ... $\mathbb{G}_m$, pour d'une part, calculer à partir de chaque défi $\mathbb{d}$ et de chaque réponse $\mathbb{D}$ un engagement reconstruit $\mathbb{R}'$ satisfaisant à une relation du type :

$$\mathbb{R}' \equiv \mathbb{G}_1^{\,d1} \cdot \mathbb{G}_2^{\,d2} \cdot \ldots \mathbb{G}_m^{\,dm} \cdot \mathbb{D}^{v} \bmod \mathbb{n}$$

ou à une relation du type :

$$\mathbb{R}' \equiv \mathbb{D}^{v} / \mathbb{G}_1^{\,d1} \cdot \mathbb{G}_2^{\,d2} \cdot \ldots \mathbb{G}_m^{\,dm} \cdot \bmod \mathbb{n}$$

puis d'autre part, calculer en appliquant la fonction de hachage $\mathbb{h}$ ayant comme arguments le message $\mathbb{M}$ et tout ou partie de chaque engagement reconstruit $\mathbb{R}'$, un jeton $\mathbb{T}'$.

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé $\mathbb{T}'$ au jeton $\mathbb{T}$ reçu.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée avec l'une et/ou l'autre des deux premières, le système selon l'invention est destiné à prouver la signature numérique d'un message $\mathbb{M}$, ci-après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- le message $\mathbb{M}$,
- les défis $\mathbb{d}$ et/ou les engagements $\mathbb{R}$,
- les réponses $\mathbb{D}$;

Opération de signature

Ledit système est tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au dispositif témoin par des moyens d'interconnexion et peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit système permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement $\mathbb{R}$**

A chaque appel, les moyens de calcul des engagements $\mathbb{R}$ du dispositif témoin calculent chaque engagement $\mathbb{R}$ en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement $\mathbb{R}$ au dispositif signataire, via les moyens d'interconnexion.

- **étape 2 : acte de défi $\mathbb{d}$**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage $\mathbb{h}$ ayant comme arguments le message $\mathbb{M}$ et tout ou partie de chaque engagement $\mathbb{R}$, pour calculer un train binaire et extraire de ce train binaire des défis $\mathbb{d}$ en nombre égal au nombre d'engagements $\mathbb{R}$.

- **étape 3 : acte de réponse $\mathbb{D}$**

Les moyens de réception des défis $\mathbb{d}$ du dispositif témoin, reçoivent chaque défi $\mathbb{d}$ provenant du dispositif signataire, via les moyens d'interconnexion.
Les moyens de calcul des réponses $\mathbb{D}$ du dispositif témoin, calculent les réponses $\mathbb{D}$ à partir des défis $\mathbb{d}$ en appliquant le processus spécifié ci-dessus.
Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses $\mathbb{D}$ au dispositif signataire, via les moyens d'interconnexion.

Opération de contrôle

Pour prouver l'authenticité du message $\mathbb{M}$, une entité appelée contrôleur, contrôle le message signé.
Ledit système comporte un dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant. Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif signataire.
Le dispositif signataire associé à l'entité signataire comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif signataire, pour transmettre au dispositif contrôleur, le message signé, via les moyens de connexion. Ainsi, le dispositif contrôleur dispose d'un message signé comprenant :

- le message $\mathbb{M}$,
- les défis $\mathbb{d}$ et/ou les engagements $\mathbb{R}$,
- les réponses $\mathbb{D}$;

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

• cas où le dispositif contrôleur dispose des engagements $\mathbb{R}$, des défis $\mathbb{d}$, des réponses $\mathbb{D}$,

Dans le cas où le dispositif contrôleur dispose des engagements $\mathbb{R}$, des défis $\mathbb{d}$, des réponses $\mathbb{D}$, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements $\mathbb{R}$, les défis $\mathbb{d}$ et les réponses $\mathbb{D}$ satisfont à des relations du type

$$\mathbb{R} \equiv \mathbb{G}_1^{\,\mathbb{d}1} \cdot \mathbb{G}_2^{\,\mathbb{d}2} \cdot \ldots \mathbb{G}_m^{\,\mathbb{d}m} \cdot \mathbb{D}^{\mathbb{v}} \bmod \mathbb{n}$$

ou à des relations du type :

$$\mathbb{R} \equiv \mathbb{D}^{\mathbb{v}} / \mathbb{G}_1^{\,\mathbb{d}1} \cdot \mathbb{G}_2^{\,\mathbb{d}2} \cdot \ldots \mathbb{G}_m^{\,\mathbb{d}m} \cdot \bmod \mathbb{n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message $\mathbb{M}$, les défis $\mathbb{d}$ et les engagements $\mathbb{R}$ satisfont à la fonction de hachage

$$\mathbb{d} = \mathbb{h}\ (\mathbb{message}, \mathbb{R})$$

• cas où le dispositif contrôleur dispose des défis $\mathbb{d}$ et des réponses $\mathbb{D}$

Dans le cas où le dispositif contrôleur dispose des défis $\mathbb{d}$ et des réponses $\mathbb{D}$, les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi $\mathbb{d}$ et de chaque réponse $\mathbb{D}$, des engagements $\mathbb{R}'$ satisfaisant à des relations du type :

$$\mathbb{R}' \equiv \mathbb{G}_1^{\,\mathbb{d}1} \cdot \mathbb{G}_2^{\,\mathbb{d}2} \cdot \ldots \mathbb{G}_m^{\,\mathbb{d}m} \cdot \mathbb{D}^{\mathbb{v}} \bmod \mathbb{n}$$

ou à des relations du type :

$$\mathbb{R}' \equiv \mathbb{D}^{\mathbb{v}} / \mathbb{G}_1^{\,\mathbb{d}1} \cdot \mathbb{G}_2^{\,\mathbb{d}2} \cdot \ldots \mathbb{G}_m^{\,\mathbb{d}m} \cdot \bmod \mathbb{n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message $\mathbb{M}$ et les défis $\mathbf{d}$ satisfont à la fonction de hachage

$$\mathbf{d = h\ (message, \mathbb{R}')}$$

◦ cas où le dispositif contrôleur dispose des engagements $\mathbb{R}$ et des réponses $\mathbb{D}$

Dans le cas où le dispositif contrôleur dispose des engagements $\mathbb{R}$ et des réponses $\mathbb{D}$, les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent $\mathbf{d'}$ tel que

$$\mathbf{d' = h\ (message, \mathbb{R})}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements $\mathbb{R}$, les défis $\mathbf{d'}$ et les réponses $\mathbb{D}$, satisfont à des relations du type :

$$\mathbb{R} \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \mathbb{D}^v \bmod n$$

ou à des relations du type :

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \bmod n$$

Dispositif Terminal

L'invention concerne aussi un dispositif terminal associé à une entité. Le dispositif terminal se présente notamment sous la forme d'un objet nomade par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif terminal est destiné à prouver à un dispositif contrôleur :

- l'authenticité de l'entité et/ou
- l'intégrité d'un message $\mathbb{M}$ associé à cette entité.

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- $\mathbb{m}$ couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$ ($\mathbb{m}$ étant supérieur ou égal à 1),
- un module public $\mathbb{n}$ constitué par le produit de $\mathbb{f}$ facteurs premiers $p_1, p_2, \ldots p_f$ ($\mathbb{f}$ étant supérieur ou égal à 2),
- un exposant public $\mathbb{v}$.

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n .$$

Ledit exposant v est tel que

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1 .

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers $p_1, p_2, \ldots p_f$. Le nombre de base g_i est tel que :

les deux équations :

$$x^2 \equiv g_i \mathbf{mod}\ n \quad \text{et} \quad x^2 \equiv -g_i \mathbf{mod}\ n$$

n'ont pas de solution en x dans l'anneau des entiers modulo n

et tel que :

l'équation :

$$x^v \equiv g_i^2 \mathbf{mod}\ n$$

a des solutions en x dans l'anneau des entiers modulo n .

Ledit dispositif terminal comprend un dispositif témoin comportant une zone mémoire contenant les f facteurs premiers p_i et/ou les paramètres des restes chinois des facteurs premiers et/ou le module public n et/ou les m valeurs privées Q_i et/ou les $f.m$ composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs privées Q_i et l'exposant public v .

Ledit dispositif témoin comporte aussi :

- des moyens de production d'aléas, ci-après désignés les moyens de production d'aléas du dispositif témoin,

- des moyens de calcul, ci-après désignés les moyens de calcul des engagements R du dispositif témoin, pour calculer des engagements R dans l'anneau des entiers modulo n .

Chaque engagement est calculé :

◦ soit en effectuant des opérations du type

$$R \equiv r^v \mathbf{mod}\ n$$

ou r est un aléa produit par les moyens de production d'aléas, r étant tel que $0 < r < n$,

- soit en effectuant des opérations du type

$$R_i \equiv r_i^{\,v} \bmod p_i$$

ou r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, \ldots r_f\}$ produits par les moyens de production d'aléas, puis en appliquant la méthode des restes chinois.

Le dispositif témoin comporte aussi :

- des moyens de réception, ci-après désignés les moyens de réception des défis d du dispositif témoin, pour recevoir un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ;

- des moyens de calcul, ci après désignés les moyens de calcul des réponses D du dispositif témoin, pour calculer à partir de chaque défi d une réponse D,

- soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{\,d1} \cdot Q_2^{\,d2} \cdot \ldots Q_m^{\,dm} \bmod n$$

- soit en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod p_i$$

puis en appliquant la méthode des restes chinois.

Ledit dispositif témoin comporte aussi des moyens de transmission pour transmettre un ou plusieurs engagements R et une ou plusieurs réponses D. Il y a autant de réponses D que de défis d que d'engagements R. Chaque groupe de nombres R, d, D constituant un triplet noté {R, d, D}.

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le dispositif terminal selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif terminal est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur. Ledit dispositif démonstrateur est

interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur.

Ledit dispositif démonstrateur comporte aussi des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement $\mathbb{R}$**

A chaque appel, les moyens de calcul des engagements $\mathbb{R}$ du dispositif témoin calculent chaque engagement $\mathbb{R}$ en appliquant le processus spécifié ci-dessus.

Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement $\mathbb{R}$ au dispositif démonstrateur, via les moyens d'interconnexion. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du démonstrateur, pour transmettre tout ou partie de chaque engagement $\mathbb{R}$ au dispositif contrôleur, via les moyens de connexion.

- **étapes 2 et 3 : acte de défi $\mathbb{d}$, acte de réponse $\mathbb{D}$**

Les moyens de réception des défis $\mathbb{d}$ du dispositif témoin, reçoivent chaque défi $\mathbb{d}$ provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin. Les moyens de calcul des réponses $\mathbb{D}$ du dispositif témoin, calculent les réponses $\mathbb{D}$ à partir des défis $\mathbb{d}$ en appliquant le processus spécifié ci-

dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse $\mathbb{D}$ au dispositif contrôleur qui procède au contrôle.

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée à la première, le dispositif terminal selon l'invention est destiné à prouver à une entité appelée contrôleur l'intégrité d'un message $\mathbb{M}$ associé à une entité appelée démonstrateur. Ledit dispositif terminal est tel qu'il comporte un dispositif démonstrateur associé à l'entité démonstrateur, ledit dispositif démonstrateur est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit dispositif démonstrateur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement $\mathbb{R}$**

A chaque appel, les moyens de calcul des engagements $\mathbb{R}$ du dispositif témoin calculent chaque engagement $\mathbb{R}$ en appliquant le processus spécifié ci-dessus Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement $\mathbb{R}$ au dispositif démonstrateur, via les moyens d'interconnexion.

- **étapes 2 et 3 : acte de défi d, acte de réponse $\mathbb{D}$**

Le dispositif démonstrateur comporte des moyens de calcul, ci-après désignés les moyens de calcul du démonstrateur, appliquant une fonction de hachage $\mathbb{h}$ ayant comme arguments le message $\mathbb{M}$ et tout ou partie de chaque engagement $\mathbb{R}$, pour calculer au moins un jeton $\mathbb{T}$. Le dispositif démonstrateur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du dispositif démonstrateur, pour transmettre chaque jeton $\mathbb{T}$, via les moyens de connexion, au dispositif contrôleur.

Ledit dispositif contrôleur produit, après avoir reçu le jeton $\mathbb{T}$, des défis $\mathbb{d}$ en nombre égal au nombre d'engagements $\mathbb{R}$.

Les moyens de réception des défis $\mathbb{d}$ du dispositif témoin, reçoivent chaque défi $\mathbb{d}$ provenant du dispositif contrôleur via les moyens de connexion entre le dispositif contrôleur et le dispositif démonstrateur et via les moyens d'interconnexion entre le dispositif démonstrateur et le dispositif témoin.

Les moyens de calcul des réponses $\mathbb{D}$ du dispositif témoin calculent les réponses $\mathbb{D}$ à partir des défis $\mathbb{d}$ en appliquant le processus spécifié ci-dessus.

- **étape 4 : acte de contrôle**

Les moyens de transmission du démonstrateur transmettent chaque réponse $\mathbb{D}$ au dispositif contrôleur qui procède au contrôle.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée avec l'une ou l'autre des deux premières, le dispositif terminal selon l'invention est destiné à produire la signature numérique d'un message $\mathbb{M}$, ci-après désigné le message signé, par une entité appelée entité signataire.

Le message signé comprend :

- le message $\mathbb{M}$,
- les défis $\mathbb{d}$ et/ou les engagements $\mathbb{R}$,
- les réponses $\mathbb{D}$.

Ledit dispositif terminal est tel qu'il comporte un dispositif signataire associé à l'entité signataire. Ledit dispositif signataire est interconnecté au dispositif témoin par des moyens d'interconnexion. Il peut se présenter notamment sous la forme de microcircuits logiques dans un objet nomade par exemple sous la forme d'un microprocesseur dans une carte bancaire à microprocesseur. Ledit dispositif signataire comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, au dispositif contrôleur associé à l'entité contrôleur. Ledit dispositif contrôleur se présente notamment sous la forme d'un terminal ou d'un serveur distant.

Opération de signature

Ledit dispositif terminal permet d'exécuter les étapes suivantes :

- **étape 1 : acte d'engagement $\mathbb{R}$**

A chaque appel, les moyens de calcul des engagements $\mathbb{R}$ du dispositif témoin calculent chaque engagement $\mathbb{R}$ en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre tout ou partie de chaque engagement $\mathbb{R}$ au dispositif signataire, via les moyens d'interconnexion.

- **étape 2 : acte de défi $\mathbb{d}$**

Le dispositif signataire comporte des moyens de calcul, ci-après désignés les moyens de calcul du dispositif signataire, appliquant une fonction de hachage $\mathbb{h}$ ayant comme arguments le message $\mathbb{M}$ et tout ou partie de chaque engagement $\mathbb{R}$, pour calculer un train binaire et extraire de ce train binaire des défis $\mathbb{d}$ en nombre égal au nombre d'engagements $\mathbb{R}$.

- **étape 3 : acte de réponse $\mathbb{D}$**

Les moyens de réception des défis $\mathbb{d}$ du dispositif témoin reçoivent chaque défi $\mathbb{d}$ provenant du dispositif signataire, via les moyens d'interconnexion.

Les moyens de calcul des réponses $\mathbb{D}$ du dispositif témoin, calculent les réponses $\mathbb{D}$ à partir des défis $\mathbb{d}$ en appliquant le processus spécifié ci-dessus. Le dispositif témoin comporte des moyens de transmission, ci-après désignés les moyens de transmission du dispositif témoin, pour transmettre les réponses $\mathbb{D}$ au dispositif signataire, via les moyens d'interconnexion.

Dispositif contrôleur

L'invention concerne aussi un dispositif contrôleur. Le dispositif contrôleur peut se présenter notamment sous la forme d'un terminal ou d'un serveur distant associé à une entité contrôleur. Le dispositif contrôleur est destiné à contrôler :

- l'authenticité d'une entité et/ou
- l'intégrité d'un message $\mathbb{M}$ associé à cette entité,

Cette preuve est établie au moyen de tout ou partie des paramètres suivants ou dérivés de ceux-ci:

- $\mathbb{m}$ couples de valeurs publiques $G_1, G_2, \ldots G_m$ ($\mathbb{m}$ étant supérieur ou égal à 1),
- un module public $\mathbb{n}$ constitué par le produit de $\mathbb{f}$ facteurs premiers $p_1, p_2, \ldots p_f$ ($\mathbb{f}$ étant supérieur ou égal à 2) inconnus du dispositif contrôleur et de l'entité contrôleur associé,
- un exposant public $\mathbb{v}$.

Ledit module, ledit exposant et lesdites valeurs sont liés par des relations du type :

$$G_i \cdot Q_i^{\mathbb{v}} \equiv 1 \ . \ \mathbb{mod}\ \mathbb{n} \text{ ou } G_i \equiv Q_i^{\mathbb{v}} \ \mathbb{mod}\ \mathbb{n} \ ;$$

où Q_i désigne une valeur privée, inconnue du dispositif contrôleur, associée à la valeur publique G_i .

L'exposant $\mathbb{v}$ est tel que

$$\mathbb{v} = 2^{\mathbb{k}}$$

où $\mathbb{k}$ est un paramètre de sécurité plus grand que 1.

Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur

aux f facteurs premiers $p_1, p_2, \ldots p_f$. Le nombre de base g_i est tel que :

les deux équations :

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo n

et tel que :

l'équation :

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo n.

Cas de la preuve de l'authenticité d'une entité

Dans une première variante de réalisation le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité d'une entité appelée démonstrateur à une entité appelée contrôleur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur.

Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

- **étapes 1 et 2 : acte d'engagement $\mathbb{R}$, acte de défi d**

Ledit dispositif contrôleur comporte aussi des moyens de réception de tout ou partie des engagements $\mathbb{R}$ provenant du dispositif démonstrateur, via les moyens de connexion.

Le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu tout ou partie de chaque engagement $\mathbb{R}$, des défis d en nombre égal au nombre d'engagements $\mathbb{R}$, chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires.

Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis d au démonstrateur, via les moyens de connexion.

∘ étapes 3 et 4 : acte de réponse $\mathbb{D}$, acte de contrôle

Ledit dispositif contrôleur comporte aussi :

- des moyens de réception des réponses $\mathbb{D}$ provenant du dispositif démonstrateur, via les moyens de connexion
- des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur,
- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

Premier cas : le démonstrateur a transmis une partie de chaque engagement $\mathbb{R}$

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus une partie de chaque engagement $\mathbb{R}$, les moyens de calcul du dispositif contrôleur, disposant des m valeurs publiques $G_1, G_2, \ldots G_m$, calculent à partir de chaque défi d et de chaque réponse $\mathbb{D}$ un engagement reconstruit $\mathbb{R}'$ satisfaisant à une relation du type :

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

ou à une relation du type,

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n ,$$

Les moyens de comparaison du dispositif contrôleur comparent chaque engagement reconstruit $\mathbb{R}'$ à tout ou partie de chaque engagement $\mathbb{R}$ reçu.

Deuxième cas : le démonstrateur a transmis l'intégralité de chaque engagement $\mathbb{R}$

Dans le cas où les moyens de réception du dispositif contrôleur ont reçus l'intégralité de chaque engagement $\mathbb{R}$, les moyens de calcul et les moyens de comparaison du dispositif contrôleur, disposant des m valeurs publiques $G_1, G_2, \ldots G_m$, vérifient que chaque engagement $\mathbb{R}$ satisfait à une relation du type :

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

ou à une relation du type,

$$\mathbb{R} \equiv \mathbb{D}^{v} / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathrm{mod}\, n .$$

Cas de la preuve de l'intégrité d'un message

Dans une deuxième variante de réalisation susceptible d'être combinée avec la première, le dispositif contrôleur selon l'invention est destiné à prouver l'intégrité d'un message $\mathbb{M}$ associé à une entité appelée démonstrateur.

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif démonstrateur associée à l'entité démonstrateur.

Ledit dispositif contrôleur permet d'exécuter les étapes suivantes :

- **étapes 1 et 2 : acte d'engagement $\mathbb{R}$, acte de défi $\mathbb{d}$**

Ledit dispositif contrôleur comporte aussi des moyens de réception de jetons $\mathbb{T}$ provenant du dispositif démonstrateur, via les moyens de connexion. Le dispositif contrôleur comporte des moyens de production de défis pour produire, après avoir reçu le jeton $\mathbb{T}$, des défis $\mathbb{d}$ en nombre égal au nombre d'engagements $\mathbb{R}$, chaque défi $\mathbb{d}$ comportant $\mathbb{m}$ entiers $\mathbb{d}_i$ ci-après appelés défis élémentaires. Le dispositif contrôleur comporte aussi des moyens de transmission, ci-après désignés les moyens de transmission du contrôleur, pour transmettre les défis $\mathbb{d}$ au démonstrateur, via les moyens de connexion.

- **étapes 3 et 4 : acte de réponse $\mathbb{D}$, acte de contrôle**

Ledit dispositif contrôleur comporte des moyens de réception des réponses $\mathbb{D}$ provenant du dispositif démonstrateur, via les moyens de connexion. Ledit dispositif contrôleur comporte aussi des moyens de calcul, ci-après désignés les moyens de calcul du dispositif contrôleur, disposant des $\mathbb{m}$ valeurs publiques G_1, G_2, ... G_m, pour d'une part, calculer à partir de chaque défi $\mathbb{d}$ et de chaque réponse $\mathbb{D}$ un engagement reconstruit $\mathbb{R}'$

satisfaisant à une relation du type :

$$\mathbb{R}' \equiv \mathbb{G}_1^{\,d1} \cdot \mathbb{G}_2^{\,d2} \cdot \ldots \mathbb{G}_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

ou à une relation du type :

$$\mathbb{R}' \equiv \mathbb{D}^v / \mathbb{G}_1^{\,d1} \cdot \mathbb{G}_2^{\,d2} \cdot \ldots \mathbb{G}_m^{\,dm} \cdot \bmod n$$

puis d'autre part, calculer en appliquant une fonction de hachage h ayant comme arguments le message $\mathbb{M}$ et tout ou partie de chaque engagement reconstruit $\mathbb{R}'$, un jeton $\mathbb{T}'$.

Le dispositif contrôleur comporte aussi des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur, pour comparer le jeton calculé $\mathbb{T}'$ au jeton $\mathbb{T}$ reçu.

Signature numérique d'un message et preuve de son authenticité

Dans une troisième variante de réalisation susceptible d'être combinée avec l'une et/ou l'autre des deux premières, le dispositif contrôleur selon l'invention est destiné à prouver l'authenticité du message $\mathbb{M}$ en contrôlant, par une entité appelée contrôleur, un message signé.

Le message signé, émis par un dispositif signataire associé à une entité signataire disposant d'une fonction de hachage h (message, $\mathbb{R}$), comprend:

- le message $\mathbb{M}$,
- des défis d et/ou des engagements $\mathbb{R}$,
- des réponses $\mathbb{D}$;

Opération de contrôle

Ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique, notamment via un réseau de communication informatique, à un dispositif signataire associée à l'entité signataire. Ledit dispositif contrôleur reçoit le message signé du dispositif signataire, via les moyens de connexion.

Le dispositif contrôleur comporte :

- des moyens de calcul, ci-après désignés les moyens de calcul du

dispositif contrôleur,

- des moyens de comparaison, ci-après désignés les moyens de comparaison du dispositif contrôleur.

◦ cas où le dispositif contrôleur dispose des engagements $\mathbb{R}$, des défis $\mathbb{d}$, des réponses $\mathbb{D}$,

Dans le cas où le dispositif contrôleur dispose des engagements $\mathbb{R}$, des défis $\mathbb{d}$, des réponses $\mathbb{D}$, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements $\mathbb{R}$, les défis $\mathbb{d}$ et les réponses $\mathbb{D}$ satisfont à des relations du type

$$\mathbb{R} \equiv \mathbb{G}_1^{\,d1} . \mathbb{G}_2^{\,d2} . \ldots \mathbb{G}_m^{\,dm} . \mathbb{D}^v \bmod \mathbb{n}$$

ou à des relations du type :

$$\mathbb{R} \equiv \mathbb{D}^v / \mathbb{G}_1^{\,d1} . \mathbb{G}_2^{\,d2} . \ldots \mathbb{G}_m^{\,dm} . \bmod \mathbb{n}$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message $\mathbb{M}$, les défis $\mathbb{d}$ et les engagements $\mathbb{R}$ satisfont à la fonction de hachage :

$$\mathbb{d} = \mathbb{h}\ (\text{message}, \mathbb{R})$$

◦ cas où le dispositif contrôleur dispose des défis $\mathbb{d}$ et des réponses $\mathbb{D}$

Dans le cas où le dispositif contrôleur dispose des défis $\mathbb{d}$ et des réponses $\mathbb{D}$, les moyens de calcul du dispositif contrôleur calculent, à partir de chaque défi $\mathbb{d}$ et de chaque réponse $\mathbb{D}$, des engagements $\mathbb{R}'$ satisfaisant à des relations du type :

$$\mathbb{R}' \equiv \mathbb{G}_1^{\,d1} . \mathbb{G}_2^{\,d2} . \ldots \mathbb{G}_m^{\,dm} . \mathbb{D}^v \bmod \mathbb{n}$$

ou à des relations du type :

$$\mathbb{R}' \equiv \mathbb{D}^v / \mathbb{G}_1^{\,d1} . \mathbb{G}_2^{\,d2} . \ldots \mathbb{G}_m^{\,dm} . \bmod \mathbb{n}$$

puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que le message $\mathbb{M}$ et les défis $\mathbb{d}$ satisfont à la fonction de hachage

$$\mathbb{d} = \mathbb{h}\ (\text{message}, \mathbb{R}')$$

◦ cas où le dispositif contrôleur dispose des engagements $\mathbb{R}$ et des réponses $\mathbb{D}$

Dans le cas où le dispositif contrôleur dispose des engagements $\mathbb{R}$ et des réponses $\mathbb{D}$, les moyens de calcul du dispositif contrôleur appliquent la fonction de hachage et calculent $\mathbb{d}$' tel que

$$\mathbb{d}' = \mathbb{h}\ (\mathbb{message}, \mathbb{R})$$

Puis, les moyens de calcul et de comparaison du dispositif contrôleur vérifient que les engagements $\mathbb{R}$, les défis $\mathbb{d}$' et les réponses $\mathbb{D}$, satisfont à des relations du type :

$$\mathbb{R} \equiv \mathbb{G}_1^{\,\mathbb{d}'1} \cdot \mathbb{G}_2^{\,\mathbb{d}'2} \cdot \ldots \mathbb{G}_m^{\,\mathbb{d}'m} \cdot \mathbb{D}^{\mathbb{v}} \bmod \mathbb{n}$$

ou à des relations du type :

$$\mathbb{R} \equiv \mathbb{D}^{\mathbb{v}} / \mathbb{G}_1^{\,\mathbb{d}'1} \cdot \mathbb{G}_2^{\,\mathbb{d}'2} \cdot \ldots \mathbb{G}_m^{\,\mathbb{d}'m} \cdot \bmod \mathbb{n}$$

Description

Rappelons l'objectif de la technologie GQ : l'authentification dynamique d'entités et de messages associés, ainsi que la signature numérique de messages.

La version classique de la technologie GQ fait appel à la technologie RSA. Mais, si la technologie RSA dépend bel et bien de la factorisation, cette dépendance n'est pas une équivalence, loin s'en faut, comme le démontrent les attaques dites « multiplicatives » contre diverses normes de signature numérique mettant en œuvre la technologie RSA.

Dans le cadre de la technologie GQ2, la présente partie de l'invention porte plus précisément sur l'utilisation des jeux de clés GQ2 dans le cadre de l'authentification dynamique et de la signature numérique. La technologie GQ2 ne fait pas appel à la technologie RSA. L'objectif est double : d'une part, améliorer les performances par rapport à la technologie RSA ; d'autre part, éviter les problèmes inhérents à la technologie RSA. La clé privée GQ2 est la factorisation du module n. Toute attaque au niveau de striplets GQ2 se ramène à la factorisation du module n : il y a cette fois équivalence. Avec la technologie GQ2, la charge de travail est réduite, tant pour l'entité qui signe ou qui s'authentifie que pour celle qui contrôle. Grâce à un meilleur usage du problème de la factorisation, tant en sécurité qu'en performance, la technologie GQ2 concurrence la technologie RSA.

La technologie GQ2 utilise un ou plusieurs petits nombres entiers plus grands que 1, disons m petits nombres entiers ($m \geq 1$) appelés « nombres de base » et notés par g_i. Les nombres de base étant fixés de g_1 à g_m avec $m \geq 1$, une clé publique de vérification $\langle v, n \rangle$ est choisie de la manière suivante. L'exposant public de vérification v est 2^k où k est un petit nombre entier plus grand que 1 ($k \geq 2$). Le module public n est le produit d'au moins deux facteurs premiers plus grands que les nombres de base, disons f facteurs premiers ($f \geq 2$) notés par p_j, de $p_1 \ldots p_f$. Les f facteurs premiers sont choisis

de façon à ce que le module public n ait les propriétés suivantes par rapport à chacun des m nombres de base de g_1 à g_m.

- D'une part, les équations (1) et (2) n'ont pas de solution en x dans l'anneau des entiers modulo n, c'est-à-dire que g_i et $-g_i$ sont deux résidus non quadratiques (mod n).

$$x^2 \equiv g_i \pmod{n} \qquad (1)$$

$$x^2 \equiv -g_i \pmod{n} \qquad (2)$$

- D'autre part, l'équation (3) a des solutions en x dans l'anneau des entiers modulo n.

$$x^{2^\kappa} \equiv g_i^2 \pmod{n} \qquad (3)$$

La clé publique de vérification $\langle v, n \rangle$ étant fixée selon les nombres de base de g_1 à g_m avec $m \geq 1$, chaque nombre de base g_i détermine un couple de valeurs GQ2 comprenant une valeur publique G_i et une valeur privée Q_i: soit m couples notés de G_1 Q_1 à G_m Q_m. La valeur publique G_i est le carré du nombre de base g_i: soit $G_i = g_i^2$. La valeur privée Q_i est une des solutions à l'équation (3) ou bien l'inverse (mod n) d'une telle solution.

De même que le module n se décompose en f facteurs premiers, l'anneau des entiers modulo n se décompose en f corps de Galois, de CG(p_1) à CG(p_f). Voici les projections des équations (1), (2) et (3) dans CG(p_j).

$$x^2 \equiv g_i \pmod{p_j} \qquad (1.a)$$

$$x^2 \equiv -g_i \pmod{p_j} \qquad (2.a)$$

$$x^{2^\kappa} \equiv g_i^2 \pmod{p_j} \qquad (3.a)$$

Chaque valeur privée Q_i peut se représenter de manière unique par f composantes privées, une par facteur premier : $Q_{i,j} \equiv Q_i \pmod{p_j}$. Chaque composante privée $Q_{i,j}$ est une solution à l'équation (3.a) ou bien l'inverse (mod p_j) d'une telle solution. Après que toutes les solutions possibles à chaque équation (3.a) aient été calculées, la technique des restes chinois permet d'établir toutes les valeurs possibles pour chaque valeur privée Q_i à partir de f composantes de $Q_{i,1}$ à $Q_{i,f}$: Q_i = Restes Chinois ($Q_{i,1}$, $Q_{i,2}$, … $Q_{i,f}$)

de manière à obtenir toutes les solutions possibles à l'équation (3).

Voici la technique des restes chinois : soient deux nombres entiers positifs premiers entre eux a et b tels que $0 < a < b$, et deux composantes X_a de 0 à a–1 et X_b de 0 à b–1 ; il s'agit de déterminer X = Restes Chinois (X_a, X_b), c'est-à-dire, le nombre unique X de 0 à $a.b$–1 tel que $X_a \equiv X \pmod{a}$ et $X_b \equiv X \pmod{b}$. Voici le paramètre des restes chinois : $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$. Voici l'opération des restes chinois : $\varepsilon \equiv X_b \pmod{a}$; $\delta = X_a - \varepsilon$; si δ est négatif, remplacer δ par $\delta + a$; $\gamma \equiv \alpha \,.\, \delta \pmod{a}$; $X = \gamma \,.\, b + X_b$.

Lorsque les facteurs premiers sont rangés dans l'ordre croissant, du plus petit p_1 au plus grand p_f, les paramètres des restes chinois peuvent être les suivants (il y en a f–1, c'est-à-dire, un de moins que de facteurs premiers). Le premier paramètre des restes chinois est $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$. Le second paramètre des restes chinois est $\beta \equiv \{p_1.p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$. Le i ième paramètre des restes chinois est $\lambda \equiv \{p_1.p_2. \ldots p_{i-1} \pmod{p_i}\}^{-1} \pmod{p_i}$. Et ainsi de suite. Ensuite, en f–1 opérations des restes chinois, on établit un premier résultat (mod p_2 fois p_1) avec le prèmier paramètre, puis, un second résultat (mod $p_1.p_2$ fois p_3) avec le second paramètre, et ainsi de suite, jusqu'à un résultat (mod $p_1. \ldots p_{f-1}$ fois p_f), c'est-à-dire, (mod n).

Il y a plusieurs représentations possibles de la clé privée GQ2, ce qui traduit **le polymorphisme de la clé privée GQ2**. Les diverses représentations s'avèrent équivalentes : elles se ramènent toutes à la connaissance de la factorisation du module n qui est la véritable clé privée GQ2. Si la représentation affecte bien le comportement de l'entité qui signe ou qui s'authentifie, elle n'affecte pas le comportement de l'entité qui contrôle.

Voici les trois principales représentations possibles de la clé privée GQ2. 1) La représentation classique en technologie GQ consiste à stocker m valeurs privées Q_i et la clé publique de vérification $\langle v, n \rangle$; en technologie GQ2, cette représentation est concurrencée par les deux suivantes. 2) La représentation optimale en termes de charges de travail consiste à stocker

l'exposant public v, les f facteurs premiers p_j, $m.f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois. 3) La représentation optimale en termes de taille de clé privée consiste à stocker l'exposant public v, les m nombres de base g_i et les f facteurs premiers p_j, puis, à commencer chaque utilisation en établissant ou bien m valeurs privées Q_i et le module n pour se ramener à la première représentation, ou bien $m.f$ composantes privées $Q_{i,j}$ et f–1 paramètres des restes chinois pour se ramener à la seconde.

Les entités qui signent ou s'authentifient peuvent toutes utiliser les mêmes nombres de base ; sauf contre indication, les m nombres de base de g_1 à g_m peuvent alors avantageusement être les m premiers nombres premiers.

Parce que la sécurité du mécanisme d'authentification dynamique ou de signature numérique équivaut à la connaissance d'une décomposition du module, la technologie GQ2 ne permet pas de distinguer simplement deux entités utilisant le même module. Généralement, chaque entité qui s'authentifie ou signe dispose de son propre module GQ2. Toutefois, on peut spécifier des modules GQ2 à quatre facteurs premiers dont deux sont connus d'une entité et les deux autres d'une autre.

Voici un premier jeu de clés GQ2 avec $k = 6$, soit $v = 64$, $m = 3$, soit trois nombres de base : $g_1 = 3$, $g_2 = 5$ et $g_3 = 7$, et $f = 3$, soit un module à trois facteurs premiers : deux congrus à 3 (mod 4) et un à 5 (mod 8). Notons que $g = 2$ est incompatible avec un facteur premier congru à 5 (mod 8).

p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833

p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B

p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9
02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144
CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD

$Q_{1,1}$ = 0279C60D216696CD6F7526E23512DAE090CFF879FDDE

$Q_{2,1}$ = 7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89

$Q_{3,1}$ = 6FB3B9C05A03D7CADA9A3425571EF5ECC54D7A7B6F

$Q_{1,2}$ = 0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502

$Q_{2,2}$ = 04792CE70284D16E9A158C688A7B3FEAF9C40056469E

$Q_{3,2}$ = FDC4A8E53E185A4BA793E93BEE5C636DA731BDCA4E

$Q_{1,3}$ = 07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE

$Q_{2,3}$ = 0AE8551E116A3AC089566DFDB3AE003CF174FC4E4877

$Q_{3,3}$ = 01682D490041913A4EA5B80D16B685E4A6DD88070501

Q_1 = D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8
C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A
C74D9743435AB4D7CF0FF6557

Q_2 = CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4
DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8
82288273ADE67353A5BC316C093

Q_3 = 09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A
AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197
697238537FE7A0195C5E8373EB74D

Voici un second jeu de clés GQ2, avec $k = 9$, soit $v = 512$, $m = 2$, soit deux nombres de base : $g_1 = 2$ et $g_2 = 3$, et $f = 3$, soit un module à trois facteurs premiers congrus à 3 (mod 4).

p_1 = 03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB

p_2 = 062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7

p_3 = 0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D
6698AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49
761B276A8E6B6977A21D51669D039F1D7

$Q_{1,1}$ = 0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1

$Q_{2,1}$ = 0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E

$Q_{1,2}$ = 02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A

$Q_{2,2}$ = 045ECB881387582E7C556887784D2671CA118E22FCF2

$Q_{1,3}$ = B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982

$Q_{2,3}$ = 0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB

Q_1 = 27F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C
35F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6
EDDA092D0CF108D0AB708405DA46

Q_2 = 230D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64
9C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6
F11F19874DE7DC5D1DF2A9252D

Authentification dynamique

Le mécanisme d'authentification dynamique est destiné à prouver à une entité appelée **contrôleur** l'authenticité d'une autre entité appelée **démonstrateur** ainsi que l'authenticité d'un éventuel message associé *M*, de sorte que le contrôleur s'assure qu'il s'agit bien du démonstrateur et éventuellement que lui et le démonstrateur parlent bien du même message *M*. Le message associé *M* est optionnel, ce qui signifie qu'il peut être vide.

Le mécanisme d'authentification dynamique est une séquence de quatre actes : un acte d'engagement, un acte de défi, un acte de réponse et un acte de contrôle. Le démonstrateur joue les actes d'engagement et de réponse. Le contrôleur joue les actes de défi et de contrôle.

Au sein du démonstrateur, on peut isoler un témoin, de manière à isoler les paramètres et les fonctions les plus sensibles du démonstrateur, c'est-à-dire, la production des engagements et des réponses. Le témoin dispose du paramètre *k* et de la clé privée GQ2, c'est-à-dire, de la factorisation du module *n* selon l'une des trois représentations évoquées ci-dessus : ◦ les *f* facteurs premiers et les *m* nombres de base, ◦ les *m.f* composantes privées, les *f* facteurs premiers et *f*–1 paramètres des restes chinois, ◦ les *m* valeurs privées et le module *n*.

Le témoin peut correspondre à une réalisation particulière, par exemple, ◦ une carte à puce reliée à un PC formant ensemble le démonstrateur, ou

encore, ◦ des programmes particulièrement protégés au sein d'un PC, ou encore, ◦ des programmes particulièrement protégés au sein d'une carte à puce. Le témoin ainsi isolé est semblable au témoin défini ci-après au sein du signataire. A chaque exécution du mécanisme, le témoin produit un ou plusieurs engagements R, puis, autant de réponses D à autant de défis d. Chaque ensemble $\{R, d, D\}$ constitue un triplet GQ2.

Outre qu'il comprend le témoin, le démonstrateur dispose également, le cas échéant, d'une fonction de hachage et d'un message M.

Le contrôleur dispose du module n et des paramètres k et m ; le cas échéant, il dispose également de la même fonction de hachage et d'un message M'. Le contrôleur est apte à reconstituer un engagement R' à partir de n'importe quel défi d et de n'importe quelle réponse D. Les paramètres k et m renseignent le contrôleur. Faute d'indication contraire, les m nombres de base de g_1 à g_m sont les m premiers nombres premiers. Chaque défi d doit comporter m défis élémentaires notés de d_1 à d_m: un par nombre de base. Chaque défi élémentaire de d_1 à d_m doit prendre une valeur de 0 à $2^{k-1}-1$ (les valeurs de $v/2$ à $v-1$ ne sont pas utilisées). Typiquement, chaque défi est codé par m fois $k-1$ bits (et non pas m fois k bits). Par exemple, avec $k = 6$ et $m = 3$ et les nombres de base 3, 5 et 7, chaque défi comporte 15 bits transmis sur deux octets ; avec $k = 9$, $m = 2$ et les nombres de base 2 et 3, chaque défi comporte 16 bits transmis sur deux octets. Lorsque les $(k-1).m$ défis possibles sont également probables, la valeur $(k-1).m$ détermine la sécurité apportée par chaque triplet GQ2 : un imposteur qui, par définition, ne connaît pas la factorisation du module n a exactement une chance de succès sur $2^{(k-1).m}$. Lorsque $(k-1).m$ vaut de 15 à 20, un triplet suffit à assurer raisonnablement l'authentification dynamique. Pour atteindre n'importe quel niveau de sécurité, on peut produire des triplets en parallèle ; on peut également en produire en séquence, c'est-à-dire, répéter l'exécution du mécanisme.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Voici un exemple avec le premier jeu de clés avec $k = 6$.

r = B8AD426C1AC0165E94B894AC2437C1B1797EF562CFA53A4AF8
43131FF1C89CFDA1312071947 10EF9C010E8F09C60D9815121981260
919967C3E2FB4B4566088E

R = FFDD736B666F41FB771776D9D50DB7CDF03F3D976471B25C56
D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C21210C6B04
49CC4292E5DD2BDB00828AF18

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées Q_{ij}, il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i), il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Voici un exemple avec le second jeu de clés avec $k = 9$.

r_1 = B0418EABEBADF0553A28903F74472CD49EE8C82D86

R_1 = 022B365F0BEA8E157E94A9DEB0512827FFD5149880F1

r_2 = 75A8DA8FE0E60BD55D28A218E31347732339F1D667

R_2 = 057E43A242C485FC20DEEF291C774CF1B30F0163DEC2

r_3 = 0D74D2BDA5302CF8BE2F6D406249D148C6960A7D27

R_3 = 06E14C8FC4DD312BA3B475F1F40CF01ACE2A88D5BB3C

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

$$R = \text{Restes Chinois}(R_1, R_2, \ldots R_f)$$

R = 28AA7F12259BFBA81368EB49C93EEAB3F3EC6BF73B0EBD7
D3FC8395CFA1AD7FC0F9DAC169A4F6F1C46FB4C3458D1E37C9
9123B56446F6C928736B17B4BA4A529

Dans les deux cas, le démonstrateur transmet au contrôleur tout ou partie de chaque engagement $\mathbb{R}$, ou bien, un code de hachage H obtenu en hachant chaque engagement $\mathbb{R}$ et un message M.

2) L'acte de défi consiste à tirer au hasard un ou plusieurs défis d composés chacun de m défis élémentaires $d_1 \quad d_2 \ \ldots \ d_m$; chaque défi élémentaire d_i prend l'une des valeurs de 0 à $v/2-1$.

$$d = d_1 \ d_2 \ldots d_m$$

Voici un exemple pour le premier jeu de clés avec $k = 6$ et $m = 3$.

$$d_1 = 10110 = 22 = \text{'16'} \ ; \ d_2 = 00111 = 7 \ ; \ d_3 = 00010 = 2,$$
$$d = 0 \,||\, d_1 \,||\, d_2 \,||\, d_3 = 01011000\ 11100010 = 58\ \text{E2}$$

Voici un exemple pour le second jeu de clés avec $k = 9$ et $m = 2$.

$$d = d_1 \,||\, d_2 = 58\ \text{E2} = \text{soit en décimal, 88 et 226}$$

Le contrôleur transmet au démonstrateur chaque défi d.

3) L'acte de réponse comporte les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les valeurs privées selon les défis élémentaires.

$$X \equiv Q_1^{d_1}.Q_2^{d_2}...Q_m^{d_m} \pmod{n}$$
$$D \equiv r.X \pmod{n}$$

Voici un exemple pour le premier jeu de clés.

D = FF257422ECD3C7A03706B9A7B28EE3FC3A4E974AEDCDF386
5EEF38760B859FDB5333E904BBDD37B097A989F69085FE8EF6480
A2C6A290273479FEC9171990A17

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il calcule une ou plusieurs collections de f

composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$X_i \equiv Q_{1,i}^{d_1} . Q_{2,i}^{d_2} ... Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i . X_i \pmod{p_i}$$

Voici un exemple pour le second jeu de clés.

$D_1 = r_1 \cdot Q_{1,1}^{d1} \cdot Q_{2,1}^{d2} \pmod{p_1} =$
02660ADF3C73B6DC15E196152322DDE8EB5B35775E38

$D_2 = r_2 \cdot Q_{1,2}^{d1} \cdot Q_{2,2}^{d2} \pmod{p_2} =$
04C15028E5FD1175724376C11BE77052205F7C62AE3B

$D_3 = r_3 \cdot Q_{1,3}^{d1} \cdot Q_{2,3}^{d2} \pmod{p_3} =$
0903D20D0C306C8EDA9D8FB5B3BEB55E061AB39CCF52

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

D = 85C3B00296426E97897F73C7DC6341FB8FFE6E879AE12EF1F36
4CBB55BC44DEC437208CF530F8402BD9C511F5FB3B3A309257A00
195A7305C6FF3323F72DC1AB

Dans les deux cas, le démonstrateur transmet chaque réponse D au contrôleur.

4) L'acte de contrôle consiste à contrôler que chaque triplet $\{R, d, D\}$ vérifie une équation du type suivant pour une valeur non nulle,

$$R . \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k} . \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

ou bien, à rétablir chaque engagement : aucun ne doit être nul.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k} . \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Eventuellement, le contrôleur calcule ensuite un code de hachage H' en

hachant chaque engagement rétabli R' et un message M'. L'authentification dynamique est réussie lorsque le contrôleur retrouve ainsi ce qu'il a reçu à l'issue de l'acte d'engagement, c'est-à-dire, tout ou partie de chaque engagement R, ou bien, le code de hachage H.

Par exemple, une séquence d'opérations élémentaires transforme la réponse D en un engagement R'. La séquence comprend k carrés (mod n) séparés par k–1 divisions ou multiplications (mod n) par des nombres de base. Pour la i ième division ou multiplication, qui s'effectue entre le i ième carré et le i+1 ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, ... jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m.

Voici un exemple pour le premier jeu de clés.

D^2 (mod n) = FD12E8E1F1370AEC9C7BA2E05C80AD2B692D341D46F3
2B93948715491F0EB091B7606CA1E744E0688367D7BB998F7B73D5F7
FDA95D5BD6347DC8B978CA217733

$3 . D^2$ (mod n) = F739B708911166DFE715800D8A9D78FC3F332FF622D
3EAB8E7977C68AD44962BEE4DAE3C0345D1CB34526D3B67EBE8BF
987041B4852890D83FC6B48D3EF6A9DF

$3^2 . D^4$ (mod n) = 682A7AF280C49FE230BEE354BF6FFB30B7519E3C8
92DD07E5A781225BBD33920E5ADABBCD7284966D71141EAA17AF
8826635790743EA7D9A15A33ACC7491D4A7

$3^4 . D^8$ (mod n) = BE9D828989A2C184E34BA8FE0F384811642B7B548F
870699E7869F8ED851FC3DB3830B2400C516511A0C28AFDD210EC3
939E69D413F0BABC6DEC441974B1A291

$3^5 . 5 . D^8$ (mod n) = 2B40122E225CD858B26D27B768632923F2BBE5
DB15CA9EFA77EFA667E554A02AD1A1E4F6B59BD9E1AE4A537D
4AC1E89C2235C363830EBF4DB42CEA3DA98CFE00

$3^{10} . 5^2 . D^{16}$ (mod n) = BDD3B34C90ABBC870C604E27E7F2E9DB2D383
68EA46C931C66F6C7509B118E3C162811A98169C30D4DEF768397DD

B8F6526B6714218DEB627E11FACA4B9DB268

$3^{11} . 5^3 . 7 . D^{16} \pmod{n}$ = DBFA7F40D338DE4FBA73D42DBF427BBF195
C13D02AB0FA5F8C8DDB5025E34282311CEF80BACDCE5D0C433444
A2AF2B15318C36FE2AE02F3C8CB25637C9AD712F

$3^{22} . 5^6 . 7^2 . D^{32} \pmod{n}$ = C60CA9C4A11F8AA89D9242CE717E3DC6C1
A95D5D09A2278F8FEE1DFD94EE84D09D000EA8633B53C4A0E7F0A
EECB70509667A3CB052029C94EDF27611FAE286A7

$3^{22} . 5^7 . 7^2 . D^{32} \pmod{n}$ = DE40CB6B41C01E722E4F312AE7205F18CDD
0303EA52261CB0EA9F0C7E0CD5EC53D42E5CB645B6BB1A3B00C77
886F4AC5222F9C863DACA440CF5F1A8E374807AC

$3^{44} . 5^{14} . 7^4 . D^{64} \pmod{n}$, c'est-à-dire, $3^{2C} . 5^E . 7^4 . D^{40} \pmod{n}$ avec les exposants en hexa = FFDD736B666F41FB771776D9D50DB7CDF03F3D9
76471B25C56D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C
21210C6B0449CC4292E5DD2BDB00828AF18

On retrouve bien l'engagement R. L'authentification est réussie.

Voici un exemple pour le second jeu de clés.

$D^2 \pmod{n}$ = C66E585D8F132F7067617BC6D00BA699ABD74FB9D13E
24E6A6692CC8D2FC7B57352D66D34F5273C13F20E3FAA228D70AEC
693F8395ACEF9206B172A8A2C2CCBB

$3 . D^2 \pmod{n}$ = 534C6114D385C3E15355233C5B00D09C2490D1B8D8E
D3D59213CB83EAD41C309A187519E5F501C4A45C37EB2FF38FBF20
1D6D138F3999FC1D06A2B2647D48283

$3^2 . D^4 \pmod{n}$ = A9DC8DEA867697E76B4C18527DFFC49F4658473D03
4EC1DDE0EB21F6F65978BE477C4231AC9B1EBD93D5D49422408E47
15919023B16BC3C6C46A92BBD326AADF

$2 . 3^3 . D^4 \pmod{n}$ = FB2D57796039DFC4AF9199CAD44B66F257A1FF
3F2BA4C12B0A8496A0148B4DFBAFE838E0B5A7D9FB4394379D72A
107E45C51FCDB7462D03A35002D29823A2BB5

$2^2 . 3^6 . D^8 \pmod{n}$ = 4C210F96FF6C77541910623B1E49533206DFB9E91

6521F305F12C5DB054D4E1BF3A37FA293854DF02B49283B6DE5E5D
82ACB23DAF1A0D5A721A1890D03A00BD8

$2^2 . 3^7 . D^8 \pmod{n}$ = E4632EC4FE4565FC4B3126B15ADBF996149F2D
BB42F65D911D3851910FE7EA53DAEA7EE7BA8FE9D081DB78B249
B1B18880616B90D4E280F564E49B270AE02388

$2^4 . 3^{14} . D^{16} \pmod{n}$ = ED3DDC716AE3D1EA74C5AF935DE814BCC
2C78B12A6BB29FA542F9981C5D954F53D153B9F0198BA82690EF
665C17C399607DEA54E218C2C01A890D422EDA16FA3

$2^5 . 3^{14} . D^{16} \pmod{n}$ = DA7C64E0E8EDBE9CF823B71AB13F17E1161487
6B000FBB473F5FCBF5A5D8D26C7B2A05D03BDDD588164E562D0F5
7AE94AE0AD3F35C61C0892F4C91DC0B08ED6F

$2^{10} . 3^{28} . D^{32} \pmod{n}$ = 6ED6AFC5A87D2DD117B0D89072C99FB9DC9
5D558F65B6A1967E6207D4ADBBA32001D3828A35069B256A07C3D
722F17DA30088E6E739FBC419FD7282D16CD6542

$2^{11} . 3^{28} . D^{32} \pmod{n}$ = DDAD5F8B50FA5BA22F61B120E5933F73B92
BAAB1ECB6D432CFCC40FA95B77464003A705146A0D364AD40F8
7AE45E2FB460111CDCE73F78833FAE505A2D9ACA84

$2^{22} . 3^{56} . D^{64} \pmod{n}$ = A466D0CB17614EFD961000BD9EABF4F021
36F8307101882BC1764DBAACB715EFBF5D8309AE001EB5DEDA
8F000E44B3D4578E5CA55797FD4BD1F8E919BE787BD0

$2^{44} . 3^{112} . D^{128} \pmod{n}$ = 925B0EDF5047EFEC5AFABDC03A830919761
B8FBDD2BF934E2A8A31E29B976274D513007EF1269E4638B4F65F
8FDEC740778BDC178AD7AF2968689B930D5A2359

$2^{44} . 3^{113} . D^{128} \pmod{n}$ = B711D89C03FDEA8D1F889134A4F809B3F2D
8207F2AD8213D169F2E99ECEC4FE08038900F0C203B55EE4F4C803
BFB912A04F11D9DB9D076021764BC4F57D47834

$2^{88} . 3^{226} . D^{256} \pmod{n}$ = 41A83F119FFE4A2F4AC7E5597A5D0BEB4D4C
08D19E597FD034FE720235894363A19D6BC5AF323D24B1B7FCFD8D
FCC628021B4648D7EF757A3E461EF0CFF0EA13

$2^{176} . 3^{452} . D^{512} \pmod{n}$, soit $4^{88} . 9^{226} . D^{512} \pmod{n}$ = 28AA7F12259BFBA8 1368EB49C93EEAB3F3EC6BF73B0EBD7D3FC8395CFA1AD7FC0F9D AC169A4F6F1C46FB4C3458D1E37C99123B56446F6C928736B17B4BA 4A529

On retrouve bien l'engagement *R*. L'authentification est réussie.

Signature numérique

Le mécanisme de signature numérique permet à une entité appelée **signataire** de produire des messages signés et à une entité appelée **contrôleur** de vérifier des messages signés. Le message *M* est une séquence binaire quelconque : il peut être vide. Le message *M* est signé en lui adjoignant un appendice de signature qui comprend un ou plusieurs engagements et / ou défis, ainsi que les réponses correspondantes.

Le contrôleur dispose de la même fonction de hachage, des paramètres *k* et *m* et du module *n*. Les paramètres *k* et *m* renseignent le contrôleur. D'une part, chaque défi élémentaire, de d_1 à d_m, doit prendre une valeur de 0 à $2^{k-1}-1$ (les valeurs de $v/2$ à $v-1$ ne sont pas utilisées). D'autre part, chaque défi *d* doit comporter *m* défis élémentaires notés de d_1 à d_m, autant que de nombres de base. En outre, faute d'indication contraire, les *m* nombres de base, de g_1 à g_m, sont les *m* premiers nombres premiers. Avec $(k-1).m$ valant de 15 à 20, on peut signer avec quatre triplets GQ2 produits en parallèle ; avec $(k-1).m$ valant 60 ou plus, on peut signer avec un seul triplet GQ2. Par exemple, avec $k = 9$ et $m = 8$, un seul triplet GQ2 suffit ; chaque défi comporte huit octets et les nombres de base sont 2, 3, 5, 7, 11, 13, 17 et 19.

L'opération de signature est une séquence de trois actes : un acte d'engagement, un acte de défi et un acte de réponse. Chaque acte produit un ou plusieurs triplets GQ2 comprenant chacun : un engagement R ($\neq 0$), un défi *d* composé de *m* défis élémentaires notés par d_1, d_2, ... d_m et une réponse D ($\neq 0$).

Le signataire dispose d'une fonction de hachage, du paramètre *k* et de la clé

privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. Au sein du signataire, on peut isoler un témoin qui exécute les actes d'engagement et de réponse, de manière à isoler les fonctions et les paramètres les plus sensibles du démonstrateur. Pour calculer engagements et réponses, le témoin dispose du paramètre k et de la clé privée GQ2, c'est-à-dire, de la factorisation du module n selon l'une des trois représentations évoquées ci-dessus. Le témoin ainsi isolé est semblable au témoin défini au sein du démonstrateur. Il peut correspondre à une réalisation particulière, par exemple, ◦ une carte à puce reliée à un PC formant ensemble le signataire, ou encore, ◦ des programmes particulièrement protégés au sein d'un PC, ou encore, ◦ des programmes particulièrement protégés au sein d'une carte à puce.

1) L'acte d'engagement comprend les opérations suivantes.

Lorsque le témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il tire au hasard et en privé un ou plusieurs aléas r ($0 < r < n$) ; puis, par k élévations successives au carré (mod n), il transforme chaque aléa r en un engagement R.

$$R \equiv r^v \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il tire au hasard et en privé une ou plusieurs collections de f aléas : chaque collection comporte un aléa r_i par facteur premier p_i ($0 < r_i < p_i$) ; puis, par k élévations successives au carré (mod p_i), il transforme chaque aléa r_i en une composante d'engagement R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Pour chaque collection de f composantes d'engagement, le témoin établit un engagement selon la technique des restes chinois. Il y a autant d'engagements que de collections d'aléas.

$$R = \text{Restes Chinois}(R_1, R_2, \ldots R_f)$$

2) L'acte de défi consiste à hacher tous les engagements R et le message à

signer M pour obtenir un code de hachage à partir duquel le signataire forme un ou plusieurs défis comprenant chacun m défis élémentaires ; chaque défi élémentaire prend une valeur de 0 à $v/2-1$; par exemple, avec $k = 9$ et $m = 8$, chaque défi comporte huit octets. Il y a autant de défis que d'engagements.

$$d = d_1\ d_2\ \ldots\ d_m, \text{ extraits du résultat Hash}(M, R)$$

3) **L'acte de réponse** comporte les opérations suivantes.

Lorsque la témoin dispose des m valeurs privées de Q_1 à Q_m et du module n, il calcule une ou plusieurs réponses D en utilisant chaque aléa r de l'acte d'engagement et les valeurs privées selon les défis élémentaires.

$$X \equiv Q_1^{d_1}.Q_2^{d_2}...Q_m^{d_m} \pmod{n}$$

$$D \equiv r.X \pmod{n}$$

Lorsque le témoin dispose des f facteurs premiers de p_1 à p_f et des $m.f$ composantes privées $Q_{i,j}$, il calcule une ou plusieurs collections de f composantes de réponse en utilisant chaque collection d'aléas de l'acte d'engagement : chaque collection de composantes de réponse comporte une composante par facteur premier.

$$X_i \equiv Q_{1,i}^{d_1}.Q_{2,i}^{d_2}...Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i.X_i \pmod{p_i}$$

Pour chaque collection de composantes de réponse, le témoin établit une réponse selon la technique des restes chinois. Il y a autant de réponses que de défis.

$$D = \text{Restes Chinois}(D_1, D_2, \ldots D_f)$$

Le signataire signe le message M en lui adjoignant un appendice de signature comprenant :

- ou bien, chaque triplet GQ2, c'est-à-dire, chaque engagement R, chaque défi d et chaque réponse D,
- ou bien, chaque engagement R et chaque réponse D correspondante,
- ou bien, chaque défi d et chaque réponse D correspondante.

Le déroulement de l'opération de vérification dépend du contenu de l'appendice de signature. On distingue les trois cas.

Au cas où l'appendice comprend un ou plusieurs triplets, l'opération de contrôle comporte deux processus indépendants dont la chronologie est indifférente. Le contrôleur accepte le message signé si et seulement si les deux conditions suivantes sont remplies.

D'une part, chaque triplet doit être cohérent (une relation appropriée du type suivant doit être vérifiée) et recevable (la comparaison doit se faire sur une valeur non nulle).

$$R.\prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Par exemple, on transforme la réponse D par une séquence d'opérations élémentaires : k carrés (mod n) séparés par k–1 multiplications ou divisions (mod n) par des nombres de base. Pour la i ième multiplication ou division, qui s'effectue entre le i ième carré et le i+1 ième carré, le i ième bit du défi élémentaire d_1 indique s'il faut utiliser g_1, le i ième bit du défi élémentaire d_2 indique s'il faut utiliser g_2, … jusqu'au i ième bit du défi élémentaire d_m qui indique s'il faut utiliser g_m. On doit ainsi retrouver chaque engagement R présent dans l'appendice de signature.

D'autre part, le ou les triplets doivent être liés au message M. En hachant tous les engagements R et le message M, on obtient un code de hachage à partir duquel on doit retrouver chaque défi d.

$d = d_1\ d_2 \ldots\ d_m$, identiques à ceux extraits du résultat Hash(M, R)

Au cas où l'appendice ne comprend pas de défi, l'opération de contrôle commence par la reconstitution de un ou plusieurs défis d' en hachant tous les engagements R et le message M.

$d' = d'_1\ d'_2 \ldots\ d'_m$, extraits du résultat Hash(M, R)

Ensuite, le contrôleur accepte le message signé si et seulement si chaque triplet est cohérent (une relation appropriée du type suivant est vérifiée) et

recevable (la comparaison se fait sur une valeur non nulle).

$$R.\prod_{i=1}^{m} G_i^{d'i} \equiv D^{2^k} \pmod{n} \quad \text{ou bien} \quad R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d'i} \pmod{n}$$

Au cas où l'appendice ne comprend pas d'engagement, l'opération de contrôle commence par la reconstitution de un ou plusieurs engagements R' selon une des deux formules suivantes, celle qui est appropriée. Aucun engagement rétabli ne doit être nul.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \quad \text{ou bien} \quad R' \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Ensuite, le contrôleur doit hacher tous les engagements R' et le message M de façon à reconstituer chaque défis d.

$d = d_1\ d_2 \ldots d_m$, identiques à ceux extraits du résultat Hash(M, R')

Le contrôleur accepte le message signé si et seulement si chaque défi reconstitué est identique au défi correspondant figurant en appendice.

Dans la présente demande, on a montré qu'il existait des couples de valeurs privée Q et publique G permettant de mettre en œuvre le procédé, le système et le dispositif selon l'invention destiné à prouver l'authenticité d'une entité et/ou l'intégrité et/ou l'authenticité d'un message.

Dans la demande pendante déposée le même jour que la présente demande par France Télécom, TDF et la Société Math RiZK et ayant pour inventeurs Louis Guillou et Jean-Jacques Quisquater, on a décrit un procédé pour produire des jeux de clés GQ2, à savoir, des modules n et des couples de valeurs publique G et privée Q dans le cas où l'exposant v est égal à 2^k. Elle est incorporée ici par référence.

Revendication

1. Procédé d'authentification dynamique d'entités et de messages associés ainsi que de signature numérique de messages mettant en œuvre la technologie GQ ;
ledit procédé étant tel qu'il utilise des jeux de clés GQ produits de telle sorte que :
   - pour chaque nombre de base g_1 à g_m l'équation $x^v \equiv g_i^{-2} \pmod n$ où $v = 2^k$ a des solutions en x dans l'anneau des entiers modulo n,
   - parmi les nombres q_1 à q_m, au moins un nombre q_j est non trivial,
   - parmi les 2xm nombres $\pm g_1$ à $\pm g_m$, il y a au moins un résidu quadratique.

2. Système d'authentification dynamique d'entités et de messages associés ainsi que de signature numérique de messages mettant en œuvre la technologie GQ ;
ledit système étant tel qu'il utilise des jeux de clés GQ produits de telle sorte que
   - pour chaque nombre de base g_1 à g_m l'équation $x^v \equiv g_i^{-2} \pmod n$ où $v = 2^k$ a des solutions en x dans l'anneau des entiers modulo n,
   - parmi les nombres q_1 à q_m, au moins un nombre q_j est non trivial,
   - parmi les 2xm nombres $\pm g_1$ à $\pm g_m$, il y a au moins un résidu quadratique.

3. Procédé pour produire des jeux de clés selon la technologie GQ ;
ledit procédé étant tel que
   - pour chaque nombre de base g_1 à g_m l'équation $x^v \equiv g_i^{-2} \pmod n$ où $v = 2^k$ a des solutions en x dans l'anneau des entiers modulo n,
   - parmi les nombres q_1 à q_m, au moins un nombre q_j est non trivial,
   - parmi les 2xm nombres $\pm g_1$ à $\pm g_m$, il y a au moins un résidu quadratique.

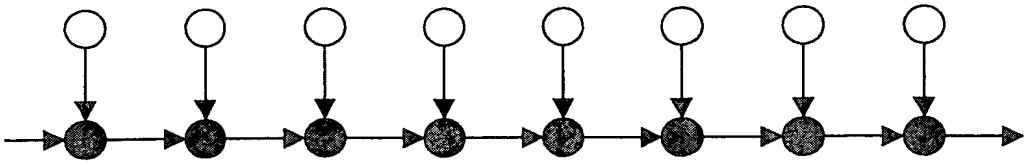

Fig.1A

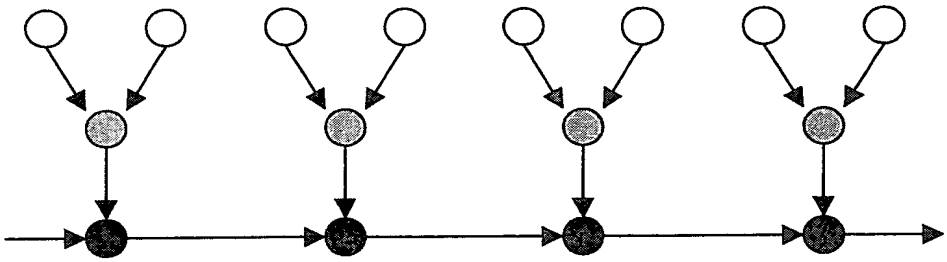

Fig.1B

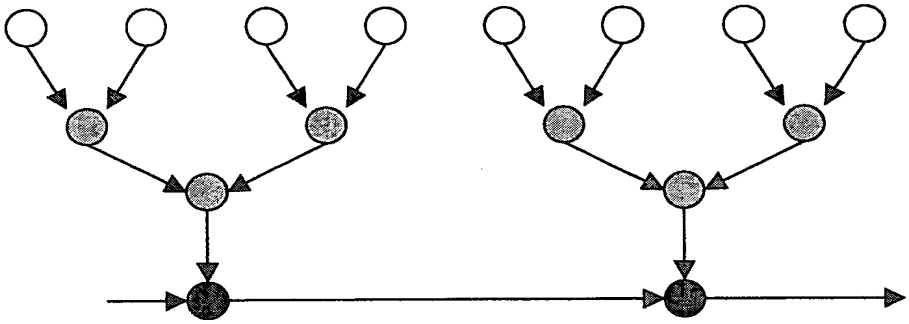

Fig.1C

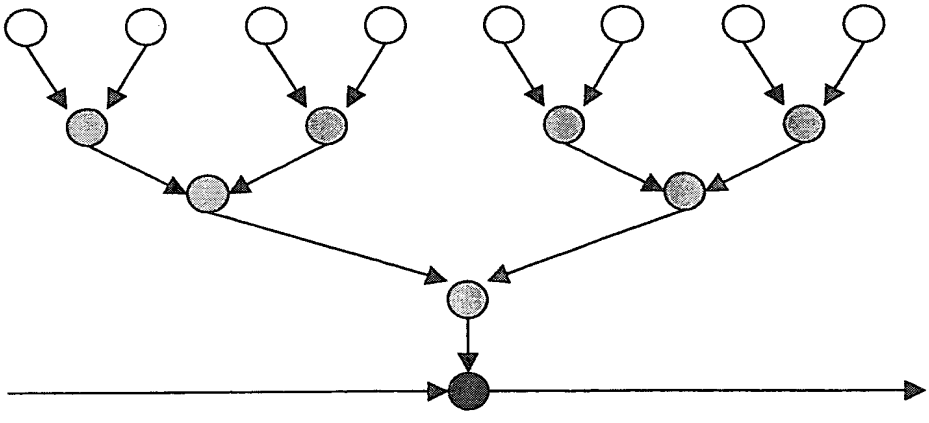

Fig.1D

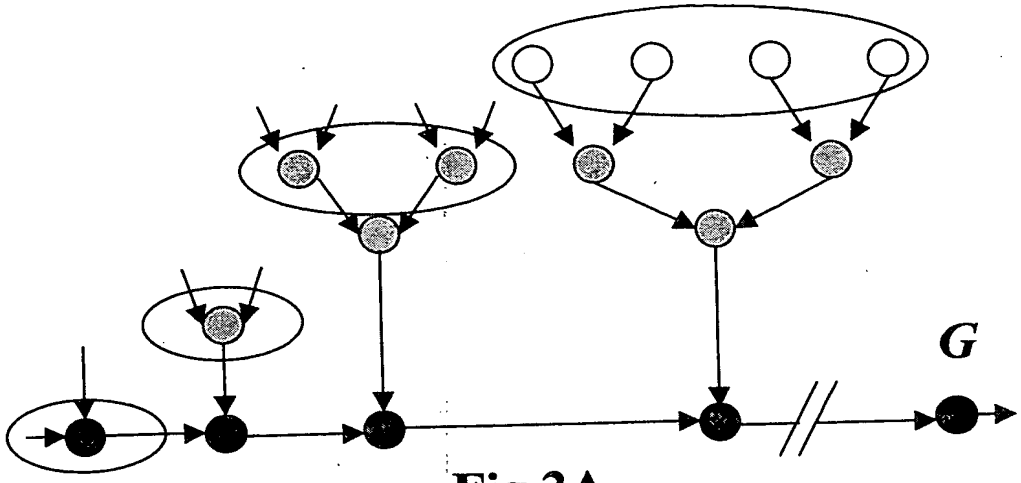

Fig.2A

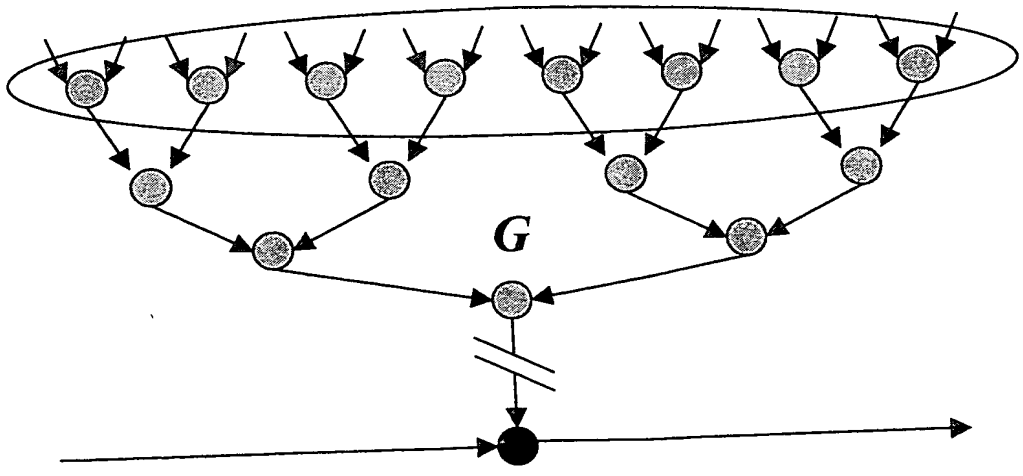

Fig.2B

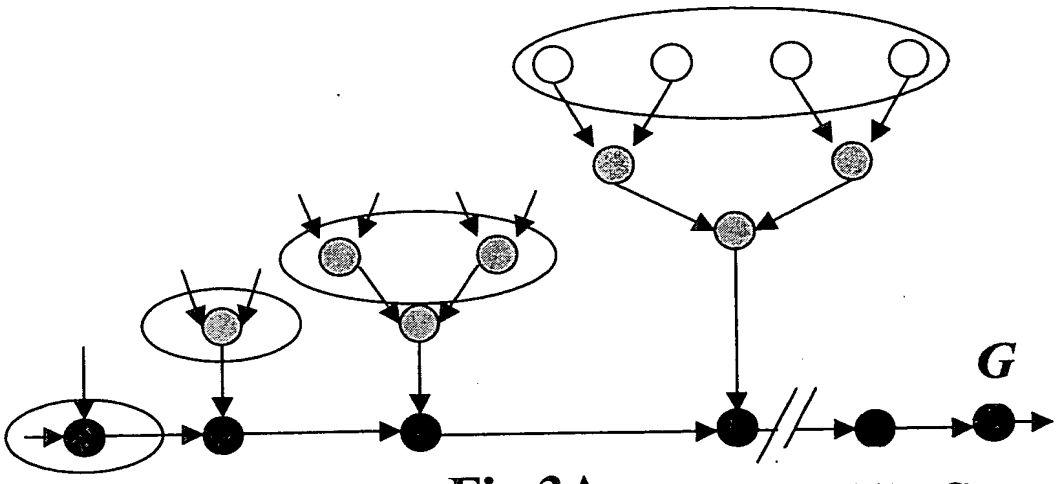

Fig.3A

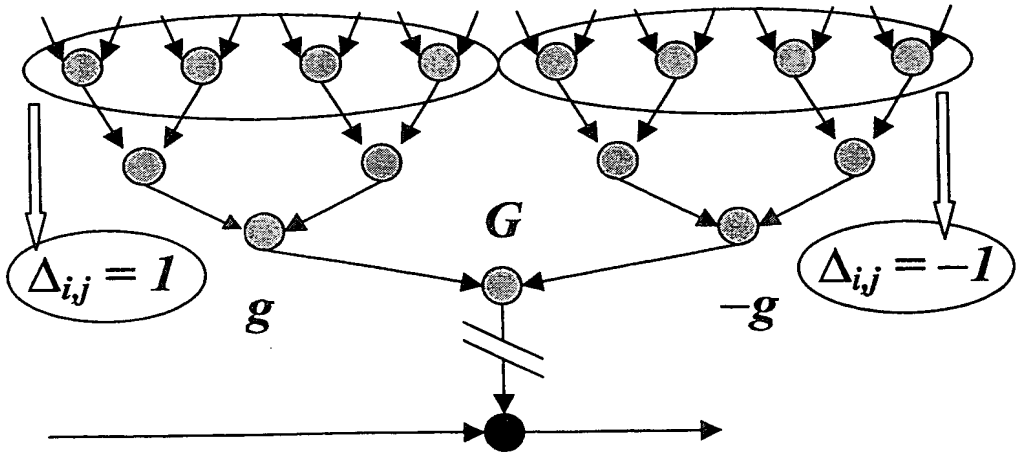

Fig.3B